Qualys. Enterprise TruRisk™ Platform

Superna Data Attack Surface Vulnerability Report

June 27, 2025

This report was generated with an evaluation version of Qualys

Report Summary	
User Name:	Andrew MacKay
Login Name:	super3am
Company:	Superna
User Role:	Manager
Address:	3630 Peachtree Road
City:	Atlanta
State:	Georgia
Zip:	30326
Country:	United States of America
Created:	06/27/2025 at 01:46:08 PM (GMT-0400)
Template Title:	High Severity Report
Asset Groups:	All
IPs:	-
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	12/31/1998 - 06/27/2025
Active Hosts:	2
Hosts Matching Filters:	1

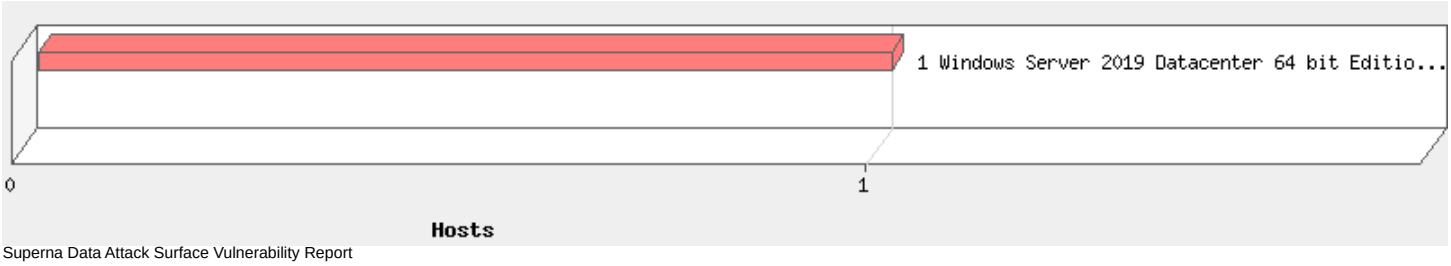
Summary of Vulnerabilities

Vulnerabilities Total	63	Security Risk (Avg)	4.1	Business Risk	39/100

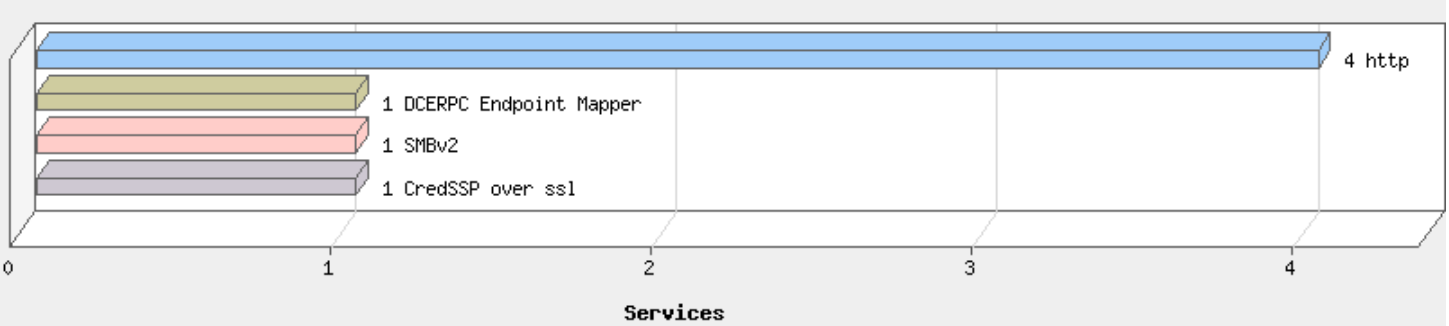
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	7	-	-	7
4	56	-	-	56
3	0	-	-	0
2	0	-	-	0
1	0	-	-	0
Total	63	-	-	63

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Local	39	-	-	39
Windows	24	-	-	24
Total	63	-	-	63

Operating Systems Detected



Services Detected



Detailed Results

10.159.10.131 (dg-win131.addg1.test, DG-WIN131) Windows Server 2019 Datacenter 64 bit Edition V...
cpe:/o:microsoft:windows_server_2019:1809::x64:

Vulnerabilities (63)

5 Microsoft Windows Server Security Update for June 2025 CVSS: 5.9 CVSS3.1: 7.9 New

QID:	92275	CVSS Base:	7.5 [1]
Category:	Windows	CVSS Temporal:	5.9
Associated CVEs:	CVE-2025-33073, CVE-2025-33057, CVE-2025-33053, CVE-2025-33075, CVE-2025-33064, CVE-2025-33061, CVE-2025-32724, CVE-2025-32720, CVE-2025-32716, CVE-2025-32715, CVE-2025-32713, CVE-2025-3052, CVE-2025-33070, CVE-2025-33069, CVE-2025-33068, CVE-2025-33056, CVE-2025-33055, CVE-2025-33052, CVE-2025-33050, CVE-2025-32725, CVE-2025-24065, CVE-2025-24069, CVE-2025-24068, CVE-2025-33071, CVE-2025-47160, CVE-2025-33067, CVE-2025-33066, CVE-2025-33065, CVE-2025-33063, CVE-2025-33062, CVE-2025-33060, CVE-2025-33059, CVE-2025-33058, CVE-2025-32722, CVE-2025-32721, CVE-2025-32719, CVE-2025-32718, CVE-2025-32714, CVE-2025-32712, CVE-2025-29828		
Vendor Reference:	KB5060842, KB5061010, KB5060531, KB5060841, KB5061078, KB5061036, KB5061026, KB5061072, KB5060118, KB5060526, KB5060525, KB5061018, KB5061059		
Bugtraq ID:	-		
Service Modified:	06/19/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft Windows Server Security Update for June 2025

KB5061078 (https://support.microsoft.com/en-in/help/5061078)
KB5061036 (https://support.microsoft.com/en-in/help/5061036)

KB5061026 (https://support.microsoft.com/en-in/help/5061026)
KB5061072 (https://support.microsoft.com/en-in/help/5061072)
KB5061010 (https://support.microsoft.com/en-in/help/5061010)
KB5060842 (https://support.microsoft.com/en-in/help/5060842)
KB5060841 (https://support.microsoft.com/en-in/help/5060841)
KB5060118 (https://support.microsoft.com/en-in/help/5060118)
KB5060526 (https://support.microsoft.com/en-in/help/5060526)
KB5060525 (https://support.microsoft.com/en-in/help/5060525)
KB5060531 (https://support.microsoft.com/en-in/help/5060531)
KB5061018 (https://support.microsoft.com/en-in/help/5061018)
KB5061059 (https://support.microsoft.com/en-in/help/5061059)

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or may affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to refer following articles for more information on the vulnerabilities and patches.

KB5061078 (https://support.microsoft.com/en-in/help/5061078)
KB5061036 (https://support.microsoft.com/en-in/help/5061036)
KB5061026 (https://support.microsoft.com/en-in/help/5061026)
KB5061072 (https://support.microsoft.com/en-in/help/5061072)
KB5061010 (https://support.microsoft.com/en-in/help/5061010)
KB5060842 (https://support.microsoft.com/en-in/help/5060842)
KB5060841 (https://support.microsoft.com/en-in/help/5060841)
KB5060118 (https://support.microsoft.com/en-in/help/5060118)
KB5060526 (https://support.microsoft.com/en-in/help/5060526)
KB5060525 (https://support.microsoft.com/en-in/help/5060525)
KB5060531 (https://support.microsoft.com/en-in/help/5060531)
KB5061018 (https://support.microsoft.com/en-in/help/5061018)
KB5061059 (https://support.microsoft.com/en-in/help/5061059)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5061078 (https://support.microsoft.com/en-in/help/5061078)

KB5061036 (https://support.microsoft.com/en-in/help/5061036)

KB5061026 (https://support.microsoft.com/en-in/help/5061026)

KB5061072 (https://support.microsoft.com/en-in/help/5061072)

KB5061010 (https://support.microsoft.com/en-in/help/5061010)

KB5060842 (https://support.microsoft.com/en-in/help/5060842)

KB5060841 (https://support.microsoft.com/en-in/help/5060841)

KB5060118 (https://support.microsoft.com/en-in/help/5060118)

KB5060526 (https://support.microsoft.com/en-in/help/5060526)

KB5060525 (https://support.microsoft.com/en-in/help/5060525)

KB5060531 (https://support.microsoft.com/en-in/help/5060531)

KB5061018 (https://support.microsoft.com/en-in/help/5061018)

KB5061059 (https://support.microsoft.com/en-in/help/5061059)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

exploitdb

Reference: CVE-2025-33073
Description: Windows 11 SMB Client - Privilege Escalation & Remote Code Execution (RCE)
Link: https://www.exploit-db.com/exploits/52330

github-exploits

Reference: CVE-2025-33073
Description: mverschu/CVE-2025-33073 exploit repository
Link: https://github.com/mverschu/CVE-2025-33073

Reference: CVE-2025-33053
Description: DevBuiHieu/CVE-2025-33053-Proof-Of-Concept exploit repository

Link: https://github.com/DevBuiHieu/CVE-2025-33053-Proof-Of-Concept

Reference: CVE-2025-33073
Description: joaozixx/CVE-2025-33073 exploit repository
Link: https://github.com/joaozixx/CVE-2025-33073

blogs

Reference: CVE-2025-33073
Description: Reflective Kerberos Relay Attack (CVE-2025-33073): NT AUTHORITY\SYSTEM Privilege Escalation
Link: https://infosecwriteups.com/reflective-kerberos-relay-attack-cve-2025-33073-nt-authority-system-privilege-escalation-bfab6cef1acc

Reference: CVE-2025-33073
Description: Authentication coercion of machine accounts and Kerberos relaying/reflection over SMB
Link: https://blog.syss.com/posts/kerberos-reflection/

Reference: CVE-2025-33073
Description: NTLM reflection is dead, long live NTLM reflection! - An in-depth analysis of CVE-2025-33073
Link: https://www.synacktiv.com/publications/ntlm-reflection-is-dead-long-live-ntlm-reflection-an-in-depth-analysis-of-cve-2025

Reference: CVE-2025-33053
Description: (CVE-2025-33053) New 0-Day in WebDAV Exposes Servers to Remote Code Execution -- Here's What You Need to Know
Link: https://infosecwriteups.com/cve-2025-33053-new-0-day-in-webdav-exposes-servers-to-remote-code-execution-heres-what-you-e1278

Reference: CVE-2025-33073
Description: NTLM reflection is dead, long live NTLM reflection! - An in-depth analysis of CVE-2025-33073
Link: https://www.synacktiv.com/en/publications/ntlm-reflection-is-dead-long-live-ntlm-reflection-an-in-depth-analysis-of-cve-2025

Reference: CVE-2025-33073
Description: A Look in the Mirror - The Reflective Kerberos Relay Attack
Link: https://blog.redteam-pentesting.de/2025/reflective-kerberos-relay-attack/

Reference: CVE-2025-3052
Description: [BRLY-2025-001] UEFI Secure Boot bypass
Link: https://www.binarly.io/advisories/brly-dva-2025-001

Reference: CVE-2025-3052
Description: Another Crack in the Chain of Trust: Uncovering (Yet Another) Secure Boot Bypass
Link: https://www.binarly.io/blog/another-crack-in-the-chain-of-trust

vulncheck-initial-access

Reference: CVE-2025-33053
Description: Microsoft Windows URL File Relative Path Local RCE
Link: https://api.vulncheck.com/v3/index/initial-access?cve=CVE-2025-33053

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Missing Patch/KB: KB5060531
File: %windir%\system32\ntoskrnl.exe
Installed Version: 10.0.17763.6292
Required Version: 10.0.17763.7434

5 Microsoft Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution (RCE) Vulnerability CVSS: 4 CVSS3.1: 8.5 New

QID:	92211	CVSS Base:	5.4 [1]
Category:	Windows	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-21307		
Vendor Reference:	KB5049984, KB5049983, KB5050063, KB5050061, KB5050048, KB5050004, KB5050049, KB5050006, KB5050013, KB5050009, KB5050021, KB5049993, KB5049981, KB5050008, CVE-2025-21307		
Bugtraq ID:	-		
Service Modified:	01/16/2025	CVSS3.1 Base:	9.8
User Modified:	-	CVSS3.1 Temporal:	8.5
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution (RCE) Vulnerability CVE-2025-21307 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21307)

An unauthenticated attacker could exploit the vulnerability by sending specially crafted packets to a Windows Pragmatic General Multicast (PGM) open socket on the server, without any interaction from the user.

Affected Operating System: Windows Server 2008, Windows 10, Windows 11, Windows Server 2025, Windows Server 2016, Windows Server version 23H2, Windows Server 2012 and Windows Server 2022.

IMPACT:

Successful exploitation of this vulnerability may allow an unauthenticated attacker to execute arbitrary code on the target system.

SOLUTION:

Vendor has released patch. Please refer to the Microsoft Security Advisory (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21307) for further information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2025-21307 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21307)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5050008 is not installed
%windir%\system32\drivers\rmcast.sys Version is 10.0.17763.6189

5 Microsoft Windows Server Security Update for January 2025 CVSS: 4.7 CVSS3.1: 9.4 New

QID:	92204	CVSS Base:	5.4 [1]
Category:	Windows	CVSS Temporal:	4.7
Associated CVEs:	CVE-2025-21217, CVE-2025-21246, CVE-2025-21334, CVE-2025-21374, CVE-2025-21340, CVE-2025-21312, CVE-2025-21292, CVE-2025-21261, CVE-2025-21227, CVE-2025-21278, CVE-2025-21189, CVE-2025-21256, CVE-2025-21228, CVE-2025-21324, CVE-2025-21317, CVE-2025-21310, CVE-2025-21287, CVE-2025-21276, CVE-2025-21211, CVE-2025-21202, CVE-2025-21207, CVE-2025-21409, CVE-2025-21223, CVE-2025-21333, CVE-2025-21332, CVE-2025-21308, CVE-2025-21232, CVE-2025-21417, CVE-2025-21339, CVE-2025-21338, CVE-2025-21286, CVE-2025-21229, CVE-2025-21193, CVE-2025-21335, CVE-2025-21330, CVE-2025-21327, CVE-2025-21238, CVE-2025-21240, CVE-2025-21331, CVE-2025-21275, CVE-2025-21273, CVE-2025-21231, CVE-2025-21226, CVE-2025-21225, CVE-2025-21224, CVE-2025-21328, CVE-2025-21341, CVE-2025-21318, CVE-2025-21245, CVE-2025-21250, CVE-2025-21313, CVE-2025-21218, CVE-2025-21305, CVE-2025-21300, CVE-2025-21274, CVE-2025-21230, CVE-2025-21213, CVE-2025-21389, CVE-2024-7344, CVE-2025-21316, CVE-2025-21315, CVE-2025-21314, CVE-2025-21326, CVE-2025-21378, CVE-2025-21372, CVE-2025-21336, CVE-2025-21323, CVE-2025-21220, CVE-2025-21329, CVE-2025-21219, CVE-2025-21321, CVE-2025-21320, CVE-2025-21319, CVE-2025-21309, CVE-2025-21306, CVE-2025-21303, CVE-2025-21299, CVE-2025-21296, CVE-2025-21293, CVE-2025-21288, CVE-2025-21270, CVE-2025-21268, CVE-2025-21263, CVE-2025-21257, CVE-2025-21251, CVE-2025-21244, CVE-2025-21242, CVE-2025-21241, CVE-2025-21236, CVE-2025-21215, CVE-2025-21382, CVE-2025-21304, CVE-2025-21302, CVE-2025-21301, CVE-2025-21298, CVE-2025-21297, CVE-2025-21295, CVE-2025-21294, CVE-2025-21291, CVE-2025-21290, CVE-2025-21289, CVE-2025-21285, CVE-2025-21284, CVE-2025-21282, CVE-2025-21281, CVE-2025-21280, CVE-2025-21277, CVE-2025-21272, CVE-2025-21271, CVE-2025-21269, CVE-2025-21266, CVE-2025-21265, CVE-2025-21260, CVE-2025-21258, CVE-2025-21255, CVE-2025-21252, CVE-2025-21249, CVE-2025-21248, CVE-2025-21243, CVE-2025-21239, CVE-2025-21237, CVE-2025-21235, CVE-2025-21234, CVE-2025-21233, CVE-2025-21214, CVE-2025-21210, CVE-2025-21413, CVE-2025-21411		
Vendor Reference:	KB5049984, KB5049983, KB5050063, KB5050061, KB5050048, KB5050004, KB5050049, KB5050006, KB5050009, KB5049993, KB5050008		
Bugtraq ID:	-		
Service Modified:	06/13/2025	CVSS3.1 Base:	9.8
User Modified:	-	CVSS3.1 Temporal:	9.4
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft Windows Server Security Update for January 2025

Affected Operating System: Windows Server 2008, Windows Server 2019, Windows Server 2016, Windows Server version 23H2, Windows Server 2012, Windows Server 2022 and Windows Server 2025.

The KB Articles associated with the update:
Patch version is 10.0.26100.2894 for KB5050009 (https://support.microsoft.com/en-in/help/5050009)
Patch version is 10.0.25398.1369 for KB5049984 (https://support.microsoft.com/en-in/help/5049984)
Patch version is 10.0.14393.7693 for KB5049993 (https://support.microsoft.com/en-in/help/5049993)
Patch version is 10.0.20348.3089 for KB5049983 (https://support.microsoft.com/en-in/help/5049983)
Patch version is 6.0.6003.23070 for KB5050063 (https://support.microsoft.com/en-in/help/5050063)
Patch version is 6.0.6003.23070 for KB5050061 (https://support.microsoft.com/en-in/help/5050061)
Patch version is 6.3.9600.22370 for KB5050048 (https://support.microsoft.com/en-in/help/5050048)
Patch version is 10.0.17763.6766 for KB5050008 (https://support.microsoft.com/en-in/help/5050008)

Patch version is 6.2.9200.25273 for KB5050004 (https://support.microsoft.com/en-in/help/5050004)
Patch version is 6.1.7601.27520 for KB5050049 (https://support.microsoft.com/en-in/help/5050049)
Patch version is 6.1.7601.27520 for KB5050006 (https://support.microsoft.com/en-in/help/5050006)

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or may affect integrity, availability, and confidentiality.

SOLUTION:

Please refer to the following KB Articles associated with the update:
KB5050009 (https://support.microsoft.com/en-in/help/5050009)
KB5049984 (https://support.microsoft.com/en-in/help/5049984)
KB5049993 (https://support.microsoft.com/en-in/help/5049993)
KB5049983 (https://support.microsoft.com/en-in/help/5049983)
KB5050063 (https://support.microsoft.com/en-in/help/5050063)
KB5050061 (https://support.microsoft.com/en-in/help/5050061)
KB5050048 (https://support.microsoft.com/en-in/help/5050048)
KB5050008 (https://support.microsoft.com/en-in/help/5050008)
KB5050004 (https://support.microsoft.com/en-in/help/5050004)
KB5050049 (https://support.microsoft.com/en-in/help/5050049)
KB5050006 (https://support.microsoft.com/en-in/help/5050006)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5050009 (https://support.microsoft.com/en-in/help/5050009)

KB5049993 (https://support.microsoft.com/en-in/help/5049993)

KB5050008 (https://support.microsoft.com/en-in/help/5050008)

KB5049984 (https://support.microsoft.com/en-in/help/5049984)

KB5049983 (https://support.microsoft.com/en-in/help/5049983)

KB5050063 (https://support.microsoft.com/en-in/help/5050063)

KB5050061 (https://support.microsoft.com/en-in/help/5050061)

KB5050048 (https://support.microsoft.com/en-in/help/5050048)

KB5050004 (https://support.microsoft.com/en-in/help/5050004)

KB5050049 (https://support.microsoft.com/en-in/help/5050049)

KB5050006 (https://support.microsoft.com/en-in/help/5050006)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

metasploit

Reference: CVE-2025-21293
Description: Windows Escalate Service Permissions Local Privilege Escalation
Link: https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/local/service_permissions.rb

github-exploits

Reference: CVE-2025-21298
Description: ynwarcs/CVE-2025-21298 exploit repository
Link: https://github.com/ynwarcs/CVE-2025-21298

Reference: CVE-2025-21333
Description: Mukesh-blend/CVE-2025-21333-POC exploit repository
Link: https://github.com/Mukesh-blend/CVE-2025-21333-POC

Reference: CVE-2025-21333
Description: 160102/CVE-2025-21333-POC exploit repository
Link: https://github.com/160102/CVE-2025-21333-POC

Reference: CVE-2025-21333
Description: SerabiLem/CVE-2025-21333-POC exploit repository
Link: https://github.com/SerabiLem/CVE-2025-21333-POC

Reference: CVE-2025-21333
Description: MrAle98/CVE-2025-21333-POC exploit repository
Link: https://github.com/MrAle98/CVE-2025-21333-POC

Reference: CVE-2025-21333
Description: B1ack4sh/Blackash-CVE-2025-21333 exploit repository
Link: https://github.com/B1ack4sh/Blackash-CVE-2025-21333

coreimpact
Reference: CVE-2025-21333
Description: Windows Hyper-V NT Kernel Integration VSP Privilege Escalation Exploit (CVE-2025-21333)
Link: https://www.coresecurity.com/core-labs/exploits

blogs
Reference: CVE-2024-7344
Description: Under the cloak of UEFI Secure Boot: Introducing CVE-2024-7344
Link: https://www.welivesecurity.com/en/eset-research/under-cloak-uefi-secure-boot-introducing-cve-2024-7344/

Reference: CVE-2025-21293
Description: Active Directory Domain Services Elevation of Privilege Vulnerability (CVE-2025-21293)
Link: https://birkep.github.io/posts/Windows-LPE/

Reference: CVE-2024-7344
Description: [One line a day] CVE-2024-7344: Secure Boot bypass due to arbitrary code execution without signature verification of Howyar Reloader UEFI application
Link: https://hackyboiz.github.io/2025/05/21/newp1ayer48/CVE-2024-7344/

ASSOCIATED MALWARE:
ReversingLabs
Malware ID: CVE-2025-21298
Type: Exploit
Platform: Win32,Document

RESULTS:

KB5050008 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.17763.6292

5 Microsoft Windows Server Security Update for November 2024 CVSS: 6.2 CVSS3.1: 9.1 New

QID:	92189	CVSS Base:	7.5 [1]
Category:	Windows	CVSS Temporal:	6.2
Associated CVEs:	CVE-2024-38203, CVE-2024-43639, CVE-2024-43629, CVE-2024-43624, CVE-2024-43620, CVE-2024-43451, CVE-2024-43450, CVE-2024-43644, CVE-2024-43637, CVE-2024-43630, CVE-2024-43628, CVE-2024-49039, CVE-2024-49019, CVE-2024-43642, CVE-2024-43641, CVE-2024-43640, CVE-2024-43636, CVE-2024-43635, CVE-2024-43622, CVE-2024-43621, CVE-2024-49046, CVE-2024-38264, CVE-2024-43452, CVE-2024-43449, CVE-2024-43447, CVE-2024-43646, CVE-2024-43645, CVE-2024-43643, CVE-2024-43638, CVE-2024-43634, CVE-2024-43631, CVE-2024-43627, CVE-2024-43626, CVE-2024-43625, CVE-2024-43623, CVE-2024-43530		
Vendor Reference:	KB5046682, KB5046697, KB5046687, KB5046705, KB5046618, KB5046661, KB5046639, KB5046616, KB5046612, KB5046615, KB5046617		
Bugtraq ID:	-		
Service Modified:	03/11/2025	CVSS3.1 Base:	9.8
User Modified:	-	CVSS3.1 Temporal:	9.1
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft Windows Server Security Update - November 2024

Patch version is 6.3.9600.22265 for KB5046682 (https://support.microsoft.com/en-in/help/5046682)
Patch version is 6.2.9200.25163 for KB5046697 (https://support.microsoft.com/en-in/help/5046697)
Patch version is 6.1.7601.27412 for KB5046687 (https://support.microsoft.com/en-in/help/5046687)
Patch version is 6.1.7601.27412 for KB5046705 (https://support.microsoft.com/en-in/help/5046705)
Patch version is 10.0.14393.7513 for KB5046612 (https://support.microsoft.com/en-in/help/5046612)
Patch version is 10.0.25398.1251 for KB5046618 (https://support.microsoft.com/en-in/help/5046618)
Patch version is 10.0.26100.2314 for KB5046617 (https://support.microsoft.com/en-in/help/5046617)
Patch version is 6.0.6003.22963 for KB5046661 (https://support.microsoft.com/en-in/help/5046661)
Patch version is 6.0.6003.22963 for KB5046639 (https://support.microsoft.com/en-in/help/5046639)
Patch version is 10.0.20348.2849 for KB5046616 (https://support.microsoft.com/en-in/help/5046616)
Patch version is 10.0.17763.6530 for KB5046615 (https://support.microsoft.com/en-in/help/5046615)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:
KB5046682 (https://support.microsoft.com/en-in/help/5046682)
KB5046697 (https://support.microsoft.com/en-in/help/5046697)
KB5046687 (https://support.microsoft.com/en-in/help/5046687)
KB5046705 (https://support.microsoft.com/en-in/help/5046705)
KB5046612 (https://support.microsoft.com/en-in/help/5046612)
KB5046618 (https://support.microsoft.com/en-in/help/5046618)
KB5046617 (https://support.microsoft.com/en-in/help/5046617)
KB5046661 (https://support.microsoft.com/en-in/help/5046661)
KB5046639 (https://support.microsoft.com/en-in/help/5046639)
KB5046616 (https://support.microsoft.com/en-in/help/5046616)
KB5046615 (https://support.microsoft.com/en-in/help/5046615)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5046682 (https://support.microsoft.com/en-in/help/5046682)

KB5046697 (https://support.microsoft.com/en-in/help/5046697)

KB5046687 (https://support.microsoft.com/en-in/help/5046687)

KB5046705 (https://support.microsoft.com/en-in/help/5046705)

KB5046612 (https://support.microsoft.com/en-in/help/5046612)

KB5046618 (https://support.microsoft.com/en-in/help/5046618)

KB5046617 (https://support.microsoft.com/en-in/help/5046617)

KB5046661 (https://support.microsoft.com/en-in/help/5046661)

KB5046639 (https://support.microsoft.com/en-in/help/5046639)

KB5046616 (https://support.microsoft.com/en-in/help/5046616)

KB5046615 (https://support.microsoft.com/en-in/help/5046615)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference: CVE-2024-49039
Description: Alexandr-bit253/CVE-2024-49039 exploit repository
Link: https://github.com/Alexandr-bit253/CVE-2024-49039

Reference: CVE-2024-43451
Description: RonF98/CVE-2024-43451-POC exploit repository
Link: https://github.com/RonF98/CVE-2024-43451-POC

Reference: CVE-2024-49019
Description: rayngnpc/CVE-2024-49019-rayng exploit repository
Link: https://github.com/rayngnpc/CVE-2024-49019-rayng

Reference: CVE-2024-49039
Description: je5442804/WPTaskScheduler_CVE-2024-49039 exploit repository
Link: https://github.com/je5442804/WPTaskScheduler_CVE-2024-49039

blogs

Reference: CVE-2024-43452
Description: Windows Kernel double-fetch in the loading of remote registry hives, leading to memory corruption
Link: https://project-zero.issues.chromium.org/issues/42451731

Reference: CVE-2024-49019
Description: EKUwu: Not just another AD CS ESC
Link: https://trustedsec.com/blog/ekuwu-not-just-another-ad-cs-esc

Reference: CVE-2024-43639
Description: CVE-2024-43639: Remote Code Execution in Microsoft Windows KDC Proxy
Link: https://www.zerodayinitiative.com/blog/2025/3/3/cve-2024-43639

Reference: CVE-2024-43451
Description: Blind Eagle: ...And Justice for All
Link: https://research.checkpoint.com/2025/blind-eagle-and-justice-for-all/

ASSOCIATED MALWARE:

ReversingLabs

Malware ID: CVE-2024-43451
Type: Exploit
Platform: Shortcut,Win32

Malware ID: CVE-2024-49039
Type: Exploit
Platform: Win64

RESULTS:

KB5046615 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.17763.6292

5 Microsoft .NET Framework Security Updates for August 2020 CVSS: 6.9 CVSS3.1: 6.8 New

QID:	91665	CVSS Base:	9.3
Category:	Windows	CVSS Temporal:	6.9
Associated CVEs:	CVE-2020-1046, CVE-2020-1476		
Vendor Reference:	KB4571692, KB4571741, KB4571709, KB4569745, KB4569746, KB4569748, KB4569749, KB4569751, KB4570500, KB4570501, KB4570502, KB4570503, KB4570505, KB4570506, KB4570507, KB4570508, KB4570509		
Bugtraq ID:	-		
Service Modified:	10/21/2021	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8

Edited: No
PCI Vuln: Yes
Ticket State:

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

.Net Framework is prone to multiple vulnerabilities.
- A remote code execution vulnerability exists when Microsoft .NET Framework processes input
- An elevation of privilege vulnerability exists when ASP.NET or .NET web applications running on IIS improperly allow access to cached files

KB4569745,KB4569746,KB4569748,KB4569749,KB4569751,KB4570500,KB4570501,KB4570502,KB4570503,KB4570505,KB4570506,KB4570507,KB4570508,KB4570509,KB4571692,KB4571709,KB4571741 kbs are covered.

This security update is rated Important or Critical for supported versions of Microsoft .NET Framework.

.NET Framework 2.0, 3.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 and 4.8

IMPACT:

An attacker who successfully exploited this vulnerability can take control of an affected system.

SOLUTION:

Customers are advised to refer to CVE-2020-1046 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1046) and CVE-2020-1476 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1476) for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2020-1046 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1046)

CVE-2020-1476 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1476)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB4569750 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\System.web.dll Version is 4.8.4110.0
%windir%\Microsoft.NET\Framework\v4.0.30319\System.web.dll Version is 4.8.4110.0

5 Microsoft SQL Server Multiple Vulnerabilities

CVSS: 5.9 CVSS3.1: 8.8 New

QID:	92029	CVSS Base:	7.5
Category:	Windows	CVSS Temporal:	5.9
Associated CVEs:	CVE-2017-15708, CVE-2015-6420		

Vendor Reference:	CVE-2015-6420, CVE-2017-15708		
Bugtraq ID:	-		
Service Modified:	06/26/2025	CVSS3.1 Base:	9.8
User Modified:	-	CVSS3.1 Temporal:	8.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft SQL Server prone to Remote Code Execution Vulnerability.

Affected Software:
SQL Server 2022 CU3
SQL Server 2019 CU19

IMPACT:

Successful exploitation could lead to remote code execution

SOLUTION:

Customers are advised to refer to
KB5024276 (https://learn.microsoft.com/en-us/troubleshoot/sql/releases/sqlserver-2019/cumulativeupdate20)
KB5024396 (https://learn.microsoft.com/en-us/troubleshoot/sql/releases/sqlserver-2022/cumulativeupdate3)
for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5024276 (https://learn.microsoft.com/en-us/troubleshoot/sql/releases/sqlserver-2019/cumulativeupdate20)

KB5024396 (https://learn.microsoft.com/en-us/troubleshoot/sql/releases/sqlserver-2022/cumulativeupdate3)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-2015-6420
Description:	Leeziao/CVE-2015-6420 exploit repository
Link:	https://github.com/Leeziao/CVE-2015-6420

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

MSSQL 2022 Version is 2022.160.1000.6 Patch Version: 2022.160.1050.5

5 Microsoft Windows Server Security Update for October 2024 CVSS: 6.2 CVSS3.1: 8.3 New

QID:	92178	CVSS Base:	7.5 [1]

Category:	Windows	CVSS Temporal:	6.2
Associated CVEs:	CVE-2024-43585, CVE-2024-43611, CVE-2024-43593, CVE-2024-43549, CVE-2024-43453, CVE-2024-38262, CVE-2024-43607, CVE-2024-43592, CVE-2024-43589, CVE-2024-43575, CVE-2024-43567, CVE-2024-43564, CVE-2024-43545, CVE-2024-43544, CVE-2024-43521, CVE-2024-43512, CVE-2024-43456, CVE-2024-38212, CVE-2024-38265, CVE-2024-38124, CVE-2024-38129, CVE-2024-38029, CVE-2024-37979, CVE-2024-43608, CVE-2024-43541, CVE-2024-38261, CVE-2024-30092, CVE-2024-37976, CVE-2024-37982, CVE-2024-37983, CVE-2024-38149, CVE-2024-43501, CVE-2024-43506, CVE-2024-43513, CVE-2024-43511, CVE-2024-43509, CVE-2024-43514, CVE-2024-43515, CVE-2024-43516, CVE-2024-43517, CVE-2024-43518, CVE-2024-43519, CVE-2024-43520, CVE-2024-43535, CVE-2024-43532, CVE-2024-43534, CVE-2024-43547, CVE-2024-43550, CVE-2024-43551, CVE-2024-43554, CVE-2024-43556, CVE-2024-43560, CVE-2024-43562, CVE-2024-43563, CVE-2024-43565, CVE-2024-43570, CVE-2024-43572, CVE-2024-43573, CVE-2024-43583, CVE-2024-43599, CVE-2024-43615, CVE-2024-6197, CVE-2024-43553, CVE-2024-38179		
Vendor Reference:	KB5044356, KB5044343, KB5044342, KB5044321, KB5044320, KB5044306, KB5044293, KB5044288, KB5044281, KB5044277		
Bugtraq ID:	-		
Service Modified:	06/08/2025	CVSS3.1 Base:	9.0
User Modified:	-	CVSS3.1 Temporal:	8.3
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft Windows Security Update - October 2024

KB5044343 (https://support.microsoft.com/en-in/help/5044343)
KB5044342 (https://support.microsoft.com/en-in/help/5044342)
KB5044356 (https://support.microsoft.com/en-in/help/5044356)
KB5044321 (https://support.microsoft.com/en-in/help/5044321)
KB5044320 (https://support.microsoft.com/en-in/help/5044320)
KB5044306 (https://support.microsoft.com/en-in/help/5044306)
KB5044293 (https://support.microsoft.com/en-in/help/5044293)
KB5044288 (https://support.microsoft.com/en-in/help/5044288)
KB5044281 (https://support.microsoft.com/en-in/help/5044281)
KB5044277 (https://support.microsoft.com/en-in/help/5044277)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:
KB5044343 (https://support.microsoft.com/en-in/help/5044343)
KB5044342 (https://support.microsoft.com/en-in/help/5044342)
KB5044356 (https://support.microsoft.com/en-in/help/5044356)
KB5044321 (https://support.microsoft.com/en-in/help/5044321)
KB5044320 (https://support.microsoft.com/en-in/help/5044320)
KB5044306 (https://support.microsoft.com/en-in/help/5044306)
KB5044293 (https://support.microsoft.com/en-in/help/5044293)
KB5044288 (https://support.microsoft.com/en-in/help/5044288)

KB5044281 (https://support.microsoft.com/en-in/help/5044281)
KB5044277 (https://support.microsoft.com/en-in/help/5044277)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5044343 (https://support.microsoft.com/en-in/help/5044343)

KB5044342 (https://support.microsoft.com/en-in/help/5044342)

KB5044356 (https://support.microsoft.com/en-in/help/5044356)

KB5044321 (https://support.microsoft.com/en-in/help/5044321)

KB5044320 (https://support.microsoft.com/en-in/help/5044320)

KB5044306 (https://support.microsoft.com/en-in/help/5044306)

KB5044293 (https://support.microsoft.com/en-in/help/5044293)

KB5044288 (https://support.microsoft.com/en-in/help/5044288)

KB5044281 (https://support.microsoft.com/en-in/help/5044281)

KB5044277 (https://support.microsoft.com/en-in/help/5044277)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-2024-43532
Description:	akamai/akamai-security-research exploit repository
Link:	https://github.com/akamai/akamai-security-research

Reference:	CVE-2024-43535
Description:	jayesther/KTM_POCS exploit repository
Link:	https://github.com/jayesther/KTM_POCS

blogs

Reference:	CVE-2024-6197
Description:	CVE-2024-6197 Curl and Libcurl: Use-after-Free on the Stack
Link:	https://jfrog.com/blog/curl-and-libcurl-uaf-cve-2024-6197/

nist-nvd2

Reference:	CVE-2024-6197
Description:	libcurl's ASN1 parser has this utf8asn1str() function used for parsing an ASN.1 UTF-8 string. Itcan detect an invalid field and return error. Unfortunately, when doing so it also invokes `free()` on a 4 byte localstack buffer. Most modern malloc implementations detect this error and immediately abort. Some however accept the input pointer and add that memory to its list of available chunks. This leads to the overwriting of nearby stack memory. The content of the overwrite is decided by the `fre
Link:	https://hackerone.com/reports/2559516

ASSOCIATED MALWARE:

ReversingLabs

Malware ID:	CVE-2024-43572
Type:	Exploit
Platform:	Script,Win32,Document

RESULTS:

KB5044277 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.17763.6292

4 Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spectre/Meltdown Variant 4)

CVSS: 1.7 CVSS3.1: 5.1 New

QID:	91462	CVSS Base:	2.1
Category:	Windows	CVSS Temporal:	1.7
Associated CVEs:	CVE-2018-3639		
Vendor Reference:	ADV180012		

Bugtraq ID:	104232		
Service Modified:	02/25/2025	CVSS3.1 Base:	5.5
User Modified:	-	CVSS3.1 Temporal:	5.1
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

On January 3 2018, Microsoft released an advisory and security updates related to hardware vulnerabilities (known as Spectre and Meltdown) involving speculative execution side channels that affect AMD, ARM, and Intel CPUs to varying degrees.
On May 21st, a new subclass of speculative execution side channel vulnerabilities known as Speculative Store Bypass (SSB) has been announced and assigned CVE-2018-3639.

The Windows registry key settings are missing on the target.
Microsoft requires you to apply the following Registry Key settings in addition to Windows Patch

To enable multiple mitigation:
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 72 /f OR REG_DWORD /d 8388680 /f OR REG_DWORD /d 8388616 /f OR REG_DWORD /d 8396872 /f OR REG_DWORD /d 8264 /f OR REG_DWORD /d 8 /f

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f

IMPACT:

An attacker who has successfully exploited this vulnerability may be able to read privileged data across trust boundaries. Vulnerable code patterns in the operating system (OS) or in applications could allow an attacker to exploit this vulnerability. In the case of Just-in-Time (JIT) compilers, such as JavaScript JIT employed by modern web browsers, it may be possible for an attacker to supply JavaScript that produces native code that could give rise to an instance of CVE-2018-3639.

SOLUTION:

Customers are advised to refer to ADV180012 (https://msrc.microsoft.com/update-guide/vulnerability/ADV180012) for more details pertaining to this vulnerability.

Please refer to the section "Enabling protections on the server" from the Microsoft link for Server Operating systems (https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution), Microsoft link for Client Operating Systems (https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in) for more details

Patch:
Following are links for downloading patches to fix the vulnerabilities:

ADV180012 (https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in)

ADV180012 (https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

 The Exploit-DB

Reference: CVE-2018-3639
Description: AMD / ARM / Intel - Speculative Execution Variant 4 Speculative Store Bypass - The Exploit-DB Ref : 44695
Link: http://www.exploit-db.com/exploits/44695

exploitdb
Reference: CVE-2018-3639
Description: AMD / ARM / Intel - Speculative Execution Variant 4 Speculative Store Bypass
Link: https://www.exploit-db.com/exploits/44695

nvd
Reference: CVE-2018-3639
Description: Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.
Link: https://www.exploit-db.com/exploits/44695/

Reference: CVE-2018-3639
Description: Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.
Link: https://bugs.chromium.org/p/project-zero/issues/detail?id=1528

packetstorm
Reference: CVE-2018-3639
Description: Speculative Execution Variant 4
Link: https://packetstormsecurity.com/files/147839/Speculative-Execution-Variant-4.html

0day.today
Reference: CVE-2018-3639
Description: AMD / ARM / Intel - Speculative Execution Variant 4 Speculative Store Bypass Exploit
Link: https://0day.today/exploit/30428

github-exploits
Reference: CVE-2018-3639
Description: Mehliug-git/PENTEST-RESEARCH exploit repository
Link: https://github.com/Mehliug-git/PENTEST-RESEARCH

coreimpact
Reference: CVE-2018-3639
Description: Speculative Store Bypass Checker (CVE-2018-3639)
Link: https://www.coresecurity.com/core-labs/exploits

nist-nvd2
Reference: CVE-2018-3639
Description: Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.
Link: https://bugs.chromium.org/p/project-zero/issues/detail?id=1528

Reference: CVE-2018-3639
Description: Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.
Link: https://www.exploit-db.com/exploits/44695/

ASSOCIATED MALWARE:

Qualys Cloud Threat DB
Malware ID: STOP
Type: Ransomware
Link: https://www.csk.gov.in/alerts/STOP_ransomware.html

Malware ID: Unattributed
Type: Ransomware

Link: https://www.csk.gov.in/alerts/STOP_ransomware.html

RESULTS:

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management FeatureSettingsOverride is missing.
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management FeatureSettingsOverrideMask is missing.

4 Microsoft Edge Based on Chromium Prior to 137.0.3296.93 Multiple Vulnerabilities CVSS: 6.7 CVSS3.1: 7.7 New

QID:	383393	CVSS Base:	9.0 [1]
Category:	Local	CVSS Temporal:	6.7
Associated CVEs:	CVE-2025-6191, CVE-2025-6192		
Vendor Reference:	Edge (chromium based) 137.0.3296.93		
Bugtraq ID:	-		
Service Modified:	06/27/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 137.0.3296.93 or later
(https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#june-20-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 137.0.3296.93 (https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#june-20-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 137.0.3296.83 Multiple Vulnerabilities CVSS: 4 CVSS3.1: 7.7 New

QID:	383361	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-5958, CVE-2025-5959		
Vendor Reference:	Edge (chromium based) 137.0.3296.83		
Bugtraq ID:	-		
Service Modified:	06/16/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 137.0.3296.83 or later (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#june-13-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 137.0.3296.83 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#june-13-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 137.0.3296.52/Extended Stable 136.0.3240.104 Multiple Vulnerabilities Multiple Vulnerabilities — CVSS: 4 CVSS3.1: 7.7 New

QID:	383322	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-5283, CVE-2025-5067, CVE-2025-5064, CVE-2025-5063, CVE-2025-5066, CVE-2025-5281, CVE-2025-5065, CVE-2025-5280		
Vendor Reference:	Edge (chromium based) 137.0.3296.52		
Bugtraq ID:	-		

Service Modified:	06/04/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 137.0.3296.52 or later (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#may-29-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 137.0.3296.52 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#may-29-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 135.0.3179.85/Extended Stable 13 4.0.3124.129 Multiple Vulnerabilities

CVSS: 4 CVSS3.1: 7.7 New

QID:	383121	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-3619, CVE-2025-3620		
Vendor Reference:	Edge (chromium based) 135.0.3179.85		
Bugtraq ID:	-		
Service Modified:	04/21/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 135.0.3179.85 or later
(https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#april-17-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 135.0.3179.85 (https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#april-17-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 135.0.3179.73 Multiple Vulnerabilities

CVSS: 4 CVSS3.1: 6.5 New

QID:	383085	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-29834		
Vendor Reference:	Edge (chromium based) 135.0.3179.73		
Bugtraq ID:	-		
Service Modified:	04/16/2025	CVSS3.1 Base:	7.5
User Modified:	-	CVSS3.1 Temporal:	6.5
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-

Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 135.0.3179.73 or later
(https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#april-11-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 135.0.3179.73 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#april-11-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 134.0.3124.66 Multiple Vulnerabilities CVSS: 4 CVSS3.1: 6.6 New

QID:	383047	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-29815		
Vendor Reference:	Edge (chromium based) 134.0.3124.66		
Bugtraq ID:	-		
Service Modified:	04/07/2025	CVSS3.1 Base:	7.6
User Modified:	-	CVSS3.1 Temporal:	6.6
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:
Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 134.0.3124.66 or later
(https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#march-12-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 134.0.3124.66 (https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#march-12-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 VMware Tools Authentication Bypass Vulnerability (VMSA-2025-0005)

CVSS: 3.4 CVSS3.1: 6.8 New

QID:	382975	CVSS Base:	4.6 [1]
Category:	Local	CVSS Temporal:	3.4
Associated CVEs:	CVE-2025-22230		
Vendor Reference:	VMSA-2025-0005		
Bugtraq ID:	-		
Service Modified:	04/23/2025	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

VMware Tools is a set of services and components that enable several features in various VMware products for better management and seamless user interactions with guest operating systems and improves management of the virtual machine running on VMware.VMware Tools for Windows contains an authentication bypass vulnerability due to improper access control.

Affected Versions:VMware Tools for Windows version 11.x.xVMware Tools for Windows version 12.x.x and prior to version 12.5.1

Affected Versions:

IMPACT:

On successful exploitation, a malicious actor with non-administrative privileges on a guest VM may gain ability to perform certain high privilege

operations within that VM.

SOLUTION:

The vendor has provided fixes in vmware tools version 12.5.1. For more information, please visit Broadcom advisory VMSA-2025-0005 (https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25518)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VMSA-2025-0005 (https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25518)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files\VMware\VMware Tools\vmtoolsd.exe Version is 12.3.0.44994

4 Microsoft Edge Based on Chromium Prior to 134.0.3124.62 Multiple Vulnerabilities

CVSS: 4.2 CVSS3.1: 7.9 New

QID:	382944	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.3
Associated CVEs:	CVE-2025-1920, CVE-2025-2135, CVE-2025-2136, CVE-2025-2137		
Vendor Reference:	Edge (chromium based) 134.0.3124.62		
Bugtraq ID:	-		
Service Modified:	06/19/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 134.0.3124.62 or later (https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#march-11-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 134.0.3124.62 (https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#march-11-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits

Reference:	CVE-2025-2135
Description:	Wa1nut4/CVE-2025-2135 exploit repository
Link:	https://github.com/Wa1nut4/CVE-2025-2135

Reference:	CVE-2025-2135
Description:	sangnguyenthien/CVE-2025-2135 exploit repository
Link:	https://github.com/sangnguyenthien/CVE-2025-2135

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 132.0.2957.115 Multiple Vulnerabilities CVSS: 7.8 CVSS3.1: 7.9 New

QID:	382691	CVSS Base:	10.0[1]
Category:	Local	CVSS Temporal:	7.8
Associated CVEs:	CVE-2025-0442, CVE-2025-0440, CVE-2025-0437, CVE-2025-0435, CVE-2025-0434, CVE-2025-0448, CVE-2025-0447, CVE-2025-0446, CVE-2025-0443, CVE-2025-0441, CVE-2025-0439, CVE-2025-0438, CVE-2025-0436, CVE-2025-21185		
Vendor Reference:	Edge (chromium based) 132.0.2957.115		
Bugtraq ID:	-		
Service Modified:	04/28/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 132.0.2957.115 or later
(https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#january-17-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 132.0.2957.115 (https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#january-17-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nist-nvd2

Reference: CVE-2025-0448
Description: Inappropriate implementation in Compositing in Google Chrome prior to 132.0.6834.83 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)
Link: https://issues.chromium.org/issues/377948403

Reference: CVE-2025-0443
Description: Insufficient data validation in Extensions in Google Chrome prior to 132.0.6834.83 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium)
Link: https://issues.chromium.org/issues/376625003

Reference: CVE-2025-0441
Description: Inappropriate implementation in Fenced Frames in Google Chrome prior to 132.0.6834.83 allowed a remote attacker to obtain potentially sensitive information from the system via a crafted HTML page. (Chromium security severity: Medium)
Link: https://issues.chromium.org/issues/368628042

Reference: CVE-2025-0434
Description: Out of bounds memory access in V8 in Google Chrome prior to 132.0.6834.83 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
Link: https://issues.chromium.org/issues/374627491

Reference: CVE-2025-0435
Description: Inappropriate implementation in Navigation in Google Chrome on Android prior to 132.0.6834.83 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: High)
Link: https://issues.chromium.org/issues/379652406

Reference: CVE-2025-0447
Description: Inappropriate implementation in Navigation in Google Chrome prior to 132.0.6834.83 allowed a remote attacker to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)
Link: https://issues.chromium.org/issues/375550814

Reference: CVE-2025-0439
Description: Race in Frames in Google Chrome prior to 132.0.6834.83 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)
Link: https://issues.chromium.org/issues/371247941

Reference: CVE-2025-0440
Description: Inappropriate implementation in Fullscreen in Google Chrome on Windows prior to 132.0.6834.83 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)
Link: https://issues.chromium.org/issues/40067914

Reference: CVE-2025-0442
Description: Inappropriate implementation in Payments in Google Chrome prior to 132.0.6834.83 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)
Link: https://issues.chromium.org/issues/40940854

Reference: CVE-2025-0436
Description: Integer overflow in Skia in Google Chrome prior to 132.0.6834.83 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
Link: https://issues.chromium.org/issues/382786791

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 131.0.2903.112/Extended Stable 130.0.2849.123 Multiple Vulnerabilities

CVSS: 4 CVSS3.1: 7.7 New

QID:	382604	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2024-12695, CVE-2024-12694, CVE-2024-12693, CVE-2024-12692		
Vendor Reference:	Edge (chromium based) 131.0.2903.112		
Bugtraq ID:	-		
Service Modified:	01/04/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 131.0.2903.112 or later (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#december-19-2024)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 131.0.2903.112 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#december-19-2024)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 131.0.2903.99/Extended Stable 130.0.2849.116 Multiple Vulnerabilities

CVSS: 4 CVSS3.1: 7.7 New

QID:	382580	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2024-12382, CVE-2024-12381		

Vendor Reference:	Edge (chromium based) 131.0.2903.99		
Bugtraq ID:	-		
Service Modified:	01/16/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 131.0.2903.99 or later (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#december-12-2024)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 131.0.2903.99 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#december-12-2024)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

 4 Microsoft Edge Based on Chromium Prior to 131.0.2903.86 Multiple Vulnerabilities CVSS: 4 CVSS3.1: 7.7 New

QID:	382524	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2024-49041, CVE-2024-12053		
Vendor Reference:	Edge (chromium based) 131.0.2903.86		
Bugtraq ID:	-		
Service Modified:	12/09/2024	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 131.0.2903.86 or later
(https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#december-5-2024)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 131.0.2903.86 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#december-5-2024)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 130.0.2849.80 Multiple Vulnerabilities CVSS: 4 CVSS3.1: 7.7 New

QID:	382316	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2024-10827, CVE-2024-10826		
Vendor Reference:	Edge (chromium based) 130.0.2849.80		
Bugtraq ID:	-		
Service Modified:	11/11/2024	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-

Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 130.0.2849.80 or later
(https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#november-7-2024)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 130.0.2849.80 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#november-7-2024)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 130.0.2849.68 Multiple Vulnerabilities CVSS: 4.3 CVSS3.1: 7.7 New

QID:	380809	CVSS Base:	5.8 [1]
Category:	Local	CVSS Temporal:	4.3
Associated CVEs:	CVE-2024-10487, CVE-2024-10488		
Vendor Reference:	Edge (chromium based) 130.0.2849.68		
Bugtraq ID:	-		
Service Modified:	11/04/2024	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:
Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 130.0.2849.68or later
(https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#october-31-2024)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 130.0.2849.68 (https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#october-31-2024)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 130.0.2849.56 Multiple Vulnerabilities CVSS: 4 CVSS3.1: 7.7 New

QID:	380787	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2024-10231, CVE-2024-10230, CVE-2024-10229		
Vendor Reference:	Edge (chromium based) 130.0.2849.56		
Bugtraq ID:	-		
Service Modified:	10/29/2024	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 130.0.2849.56 or later
(https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#october-24-2024)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 130.0.2849.56 (https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#october-24-2024)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 130.0.2849.46 Multiple Vulnerabilities CVSS: 4.2 CVSS3.1: 8.8 New

QID:	380734	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.3
Associated CVEs:	CVE-2024-43577, CVE-2024-9954, CVE-2024-9966, CVE-2024-9965, CVE-2024-9964, CVE-2024-9963, CVE-2024-9962, CVE-2024-9961, CVE-2024-9960, CVE-2024-9959, CVE-2024-9958, CVE-2024-9957, CVE-2024-9956, CVE-2024-49023, CVE-2024-9955, CVE-2024-43579, CVE-2024-43596, CVE-2024-43578, CVE-2024-43587, CVE-2024-43580, CVE-2024-43595, CVE-2024-43566		
Vendor Reference:	Edge (chromium based) 130.0.2849.46		
Bugtraq ID:	-		
Service Modified:	03/11/2025	CVSS3.1 Base:	9.8
User Modified:	-	CVSS3.1 Temporal:	8.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 130.0.2849.46 or later
(https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#october-17-2024)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 130.0.2849.46 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#october-17-2024)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd

Reference: CVE-2024-9957
Description: Use after free in UI in Google Chrome on iOS prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
Link: https://issues.chromium.org/issues/358151317

blogs

Reference: CVE-2024-9956
Description: Remote Code Execution and Critical Vulnerabilities in NASA fprime v3.4.3
Link: https://mastersplinter.work/research/passkey/

nist-nvd2

Reference: CVE-2024-9960
Description: Use after free in Dawn in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
Link: https://issues.chromium.org/issues/354748063

Reference: CVE-2024-9961
Description: Use after free in ParcelTracking in Google Chrome on iOS prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
Link: https://issues.chromium.org/issues/357776197

Reference: CVE-2024-9957
Description: Use after free in UI in Google Chrome on iOS prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)
Link: https://issues.chromium.org/issues/358151317

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 129.0.2792.89/Extended Stable 128.0.2739.113 Multiple Vulnerabilities — CVSS: 4.2 CVSS3.1: 7.9 New

QID:	380676	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.3
Associated CVEs:	CVE-2024-9603, CVE-2024-9602		
Vendor Reference:	Edge (chromium based) 129.0.2792.89		
Bugtraq ID:	-		
Service Modified:	02/08/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -

Integrity Requirement: -
Availability Requirement: -

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 129.0.2792.89 or later
(https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#october-10-2024)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 129.0.2792.89 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#october-10-2024)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nvd
Reference: CVE-2024-9602
Description: Type Confusion in V8 in Google Chrome prior to 129.0.6668.100 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)
Link: https://issues.chromium.org/issues/368241697

nist-nvd2
Reference: CVE-2024-9602
Description: Type Confusion in V8 in Google Chrome prior to 129.0.6668.100 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)
Link: https://issues.chromium.org/issues/368241697

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 129.0.2792.79/Extended Stable 128.0.2739.107 Multiple Vulnerabilities CVSS: 4.2 CVSS3.1: 8.6 New

QID:	380586	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.3
Associated CVEs:	CVE-2024-9370, CVE-2024-9369, CVE-2024-7025		
Vendor Reference:	Edge (chromium based) 129.0.2792.79		
Bugtraq ID:	-		
Service Modified:	01/04/2025	CVSS3.1 Base:	9.6
User Modified:	-	CVSS3.1 Temporal:	8.6
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 129.0.2792.79 or later
(https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#october-3-2024)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 129.0.2792.79 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#october-3-2024)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nist-nvd2

Reference: CVE-2024-7025
Description: Integer overflow in Layout in Google Chrome prior to 129.0.6668.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)
Link: https://issues.chromium.org/issues/367764861

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft SQL Server ODBC and OLE DB Driver for SQL Server Multiple Vulnerabilities for April 2024 CVSS: 3.4 CVSS3.1: 7.7 New

QID:	379596	CVSS Base:	4.6 [1]
Category:	Local	CVSS Temporal:	3.4
Associated CVEs:	CVE-2024-28906, CVE-2024-28908, CVE-2024-28909, CVE-2024-28910, CVE-2024-28911, CVE-2024-28912, CVE-2024-28913, CVE-2024-28914, CVE-2024-28915, CVE-2024-28926, CVE-2024-28927, CVE-2024-29982, CVE-2024-29983, CVE-2024-29984, CVE-2024-29985, CVE-2024-28929, CVE-2024-28930, CVE-2024-28931, CVE-2024-28932, CVE-2024-28933, CVE-2024-28934, CVE-2024-28935, CVE-2024-28936, CVE-2024-28937, CVE-2024-28938, CVE-2024-28939, CVE-2024-28940, CVE-2024-28941, CVE-2024-28942, CVE-2024-28943, CVE-2024-28944, CVE-2024-28945, CVE-2024-29043, CVE-2024-29044, CVE-2024-29045, CVE-2024-29046, CVE-2024-29047, CVE-2024-29048		
Vendor Reference:	CVE-2024-28906, CVE-2024-28908, CVE-2024-28909, CVE-2024-28910, CVE-2024-28911, CVE-2024-28912, CVE-2024-28913, CVE-2024-28914, CVE-2024-28915, CVE-2024-28926, CVE-2024-28927, CVE-2024-28929, CVE-2024-28930, CVE-2024-28931, CVE-2024-28932, CVE-2024-28933, CVE-2024-28934, CVE-2024-28935, CVE-2024-28936, CVE-2024-28937, CVE-2024-28938, CVE-2024-28939, CVE-2024-28940, CVE-2024-28941, CVE-2024-28942, CVE-2024-28943, CVE-2024-28944, CVE-2024-28945, CVE-2024-29043, CVE-2024-29044, CVE-2024-29045, CVE-2024-29046, CVE-2024-29047, CVE-2024-29048, CVE-2024-29982, CVE-2024-29983, CVE-2024-29984, CVE-2024-29985		
Bugtraq ID:	-		
Service Modified:	04/10/2024	CVSS3.1 Base:	8.8

User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

CVSS3.1 Temporal: 7.7

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft has released a security update to addressed a Remote Code Execution Vulnerability in OLE DB and ODBC driver for SQL Server. Both of these are APIs for Microsoft SQL server that provide access to a range of data sources.

Affected Software:
Microsoft ODBC Driver 17 for SQL Server on Windows version prior to 17.10.6.1
Microsoft ODBC Driver 18 for SQL Server on Windows version prior to 18.3.3.1
Microsoft ODBC Driver 17 for SQL Server on Linux version prior to 17.10.6.1
Microsoft ODBC Driver 18 for SQL Server on Linux version prior to 18.3.3.1
Microsoft SQL Server 2022 for x64-based Systems (GDR)
Microsoft SQL Server 2019 for x64-based Systems (GDR)
Microsoft SQL Server 2022 for x64-based Systems ((CU 12))
Microsoft SQL Server 2019 for x64-based Systems (CU 25)
Microsoft OLE DB Driver 19 for SQL Server version prior to 19.3.3.0
Microsoft OLE DB Driver 18 for SQL Server version prior to 18.7.2.0

IMPACT:

Successful exploitation may lead to remote code execution and denial of service.

SOLUTION:

Refer to
906 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28906)
907 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28907)
908 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28908)
909 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28909)
911 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28911)
912 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28912)
913 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28913)
914 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28914)
915 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28915)
926 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28926)
927 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28927)
929 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28929)
930 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28930)
931 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28931)
932 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28932)
933 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28933)
934 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28934)
935 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28935)
936 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28936)
937 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28937)
938 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28938)
939 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28939)
940 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28940)
941 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28941)
942 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28942)

943 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28943)
944 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28944)
945 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28945)
043 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-29043)
044 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-29044)
045 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-29045)
046 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-29046)
047 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-29047)
048 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-29048)
982 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-29982)
983 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-29983)
984 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-29984)
985 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-29985)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-28906 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28906)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

MSSQL 2022 Version is 2022.160.1000.6 Patch Version: 2022.160.1115.1

4 Microsoft SQL Server Data Provider Security Feature Bypass Vulnerability - January 2024

CVSS: 5.6 CVSS3.1: 7.6 New

QID:	379234	CVSS Base:	7.6 [1]
Category:	Local	CVSS Temporal:	5.6
Associated CVEs:	CVE-2024-0056		
Vendor Reference:	CVE-2024-0056		
Bugtraq ID:	-		
Service Modified:	11/05/2024	CVSS3.1 Base:	8.7
User Modified:	-	CVSS3.1 Temporal:	7.6
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

A successful attack could exploit a vulnerability in the SQL Data Provider which allows the attacker to exploit the SQL Server.

Affected
Software:

SQL Server 2022 CU10
SQL Server 2022 GDR

IMPACT:

An attacker who successfully exploited this vulnerability could carry out a machine-in-the-middle (MITM) attack and could decrypt and read or modify TLS traffic between the client and server.

SOLUTION:

Customers are advised to refer to
KB5033592 (https://support.microsoft.com/help/5033592)
KB5032968 (https://support.microsoft.com/help/5032968)
for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5032968 (https://support.microsoft.com/help/5032968)

KB5033592 (https://support.microsoft.com/help/5033592)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

MSSQL 2022 Version is 2022.160.1000.6 Patch Version: 2022.160.1110.1

4 VMware Tools Multiple Security Vulnerability (VMSA-2023-0024)

CVSS: 1.9 CVSS3.1: 6.8 New

QID:	378979	CVSS Base:	2.6 [1]
Category:	Local	CVSS Temporal:	1.9
Associated CVEs:	CVE-2023-34057, CVE-2023-34058		
Vendor Reference:	VMSA-2023-0024		
Bugtraq ID:	-		
Service Modified:	12/01/2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

VMware Tools is a set of services and components that enable several features in various VMware products for better management and seamless user interactions with guest operating systems and improves management of the virtual machine running on VMware.

Affected Versions:

VMware Tools for Windows version 10.3.x
VMware Tools for Windows version 11.x.x.
VMware Tools for Windows version 12.x.x and prior to version 12.3.5

Affected Versions:
VMware Tools for macOS version 10.3.x
VMware Tools for macOS version 11.x.x.
VMware Tools for macOS version 12.x.x and prior to version 12.1.1

IMPACT:

A malicious actor with local user access to a guest virtual machine may elevate privileges within the virtual machine and A malicious actor that has been granted Guest Operation Privileges in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias.

SOLUTION:

For more information please visit VMware advisory VMSA-2023-0024 (https://www.vmware.com/security/advisories/VMSA-2023-0024.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

VMSA-2023-0024 (https://www.vmware.com/security/advisories/VMSA-2023-0024.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files\VMware\VMware Tools\vmtoolsd.exe Version is 12.3.0.44994

4 Microsoft WinVerifyTrust Signature Validation Vulnerability CVSS: 6.6 CVSS3.1: 5.3 New

QID:	378332	CVSS Base:	7.6
Category:	Local	CVSS Temporal:	6.6
Associated CVEs:	CVE-2013-3900		
Vendor Reference:	CVE-2013-3900		
Bugtraq ID:	-		
Service Modified:	04/04/2025	CVSS3.1 Base:	5.5
User Modified:	-	CVSS3.1 Temporal:	5.3
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft stated that they have re-published the CVE-2013-3900 to inform customers about the availability of EnableCertPaddingCheck. This behavior remains available as an opt-in feature via the registry key setting and is available on all supported editions of Windows released since December 10, 2013.

Microsoft recommends that executable authors consider conforming all signed binaries to the new verification standard by ensuring that they contain no extraneous information in the WIN_CERTIFICATE structure. Microsoft also recommends that customers appropriately test this change to evaluate how it will behave in their environments.

Microsoft recommends that customers test how this change to Authenticode signature verification behaves in their environment before fully implementing it. To enable the Authenticode signature verification improvements, modify the registry to add the EnableCertPaddingCheck value as detailed below.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config "EnableCertPaddingCheck"="1"
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config "EnableCertPaddingCheck"="1"

IMPACT:

A remote code execution vulnerability exists in the way that the WinVerifyTrust function handles Windows Authenticode signature verification for portable executable (PE) files. An anonymous attacker could exploit the vulnerability by modifying an existing signed executable file to leverage unverified portions of the file in such a way as to add malicious code to the file without invalidating the signature.

SOLUTION:

Customers are advised to refer to WinVerifyTrust Signature Validation (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900) for further details pertaining to this.

Opting into this stricter verification behavior causes the WinVerifyTrust function to perform strict Windows Authenticode signature verification for PE files. After opting-in, PE files will be considered "unsigned" if Windows identifies content in them that does not conform to the Authenticode specification. This may impact some installers. If you are using an installer that is impacted, Microsoft recommends using an installer that only extracts content from validated portions of the signed file.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2013-3900 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits
- Reference: CVE-2013-3900
- Description: med0x2e/SigFlip exploit repository
- Link: https://github.com/med0x2e/SigFlip

cisa-kev
- Reference: CVE-2013-3900
- Description: Microsoft WinVerifyTrust function Remote Code Execution
- Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

microsoft-cvrf
- Reference: CVE-2013-3900
- Description: WinVerifyTrust Signature Validation Vulnerability
- Link: https://api.msrc.microsoft.com/cvrf/2022-Jan?api-version=2020

ASSOCIATED MALWARE:

ReversingLabs
- Malware ID: Generic
- Type: Rootkit
- Platform: Win64

- Malware ID: CVE-2013-3900
- Type: Exploit
- Platform: Win64,Win32

Qualys Cloud Threat DB

Malware ID:	Conti
Type:	Ransomware
Link:	https://blogs.vmware.com/security/2022/11/batloader-the-evasive-downloader-malware.html

RESULTS:

HKLM\Software\Microsoft\Cryptography\Wintrust\Config EnableCertPaddingCheck is missing.
HKLM\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config EnableCertPaddingCheck is missing.

4 Microsoft Windows Server Security Update for May 2025 CVSS: 4.5 CVSS3.1: 8.2 New

QID:	92260	CVSS Base:	5.4 [1]
Category:	Windows	CVSS Temporal:	4.5
Associated CVEs:	CVE-2025-32710, CVE-2025-47955, CVE-2025-47969, CVE-2025-24063, CVE-2025-30397, CVE-2025-29974, CVE-2025-29961, CVE-2025-29956, CVE-2025-29841, CVE-2025-29837, CVE-2025-29832, CVE-2025-32706, CVE-2025-27468, CVE-2025-29969, CVE-2025-29968, CVE-2025-29964, CVE-2025-32707, CVE-2025-30388, CVE-2025-30385, CVE-2025-29963, CVE-2025-29962, CVE-2025-29958, CVE-2025-29957, CVE-2025-29955, CVE-2025-29954, CVE-2025-29842, CVE-2025-29840, CVE-2025-29839, CVE-2025-29838, CVE-2025-29836, CVE-2025-29835, CVE-2025-29833, CVE-2025-29831, CVE-2025-29830, CVE-2025-29829, CVE-2025-26677, CVE-2025-32701, CVE-2025-30394, CVE-2025-29970, CVE-2025-29967, CVE-2025-29966, CVE-2025-29960, CVE-2025-29959		
Vendor Reference:	KB5058392, KB5058497, KB5058411, KB5058383, KB5058380, KB5058429, KB5058430, KB5058403, KB5058449, KB5058385, KB5058451, KB5058454, KB5058384, KB5058500		
Bugtraq ID:	-		
Service Modified:	06/10/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	8.2
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft Windows Server Security Update for May 2025

KB5058429 (https://support.microsoft.com/en-in/help/5058429)
KB5058430 (https://support.microsoft.com/en-in/help/5058430)
KB5058403 (https://support.microsoft.com/en-in/help/5058403)
KB5058449 (https://support.microsoft.com/en-in/help/5058449)
KB5058392 (https://support.microsoft.com/en-in/help/5058392)
KB5058385 (https://support.microsoft.com/en-in/help/5058385)
KB5058497 (https://support.microsoft.com/en-in/help/5058497)
KB5058451 (https://support.microsoft.com/en-in/help/5058451)
KB5058454 (https://support.microsoft.com/en-in/help/5058454)
KB5058384 (https://support.microsoft.com/en-in/help/5058384)
KB5058500 (https://support.microsoft.com/en-in/help/5058500)
KB5058411 (https://support.microsoft.com/en-in/help/5058411)
KB5058383 (https://support.microsoft.com/en-in/help/5058383)

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or may affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to refer following articles for more information on the vulnerabilities and patches.

KB5058429 (https://support.microsoft.com/en-in/help/5058429)
KB5058430 (https://support.microsoft.com/en-in/help/5058430)
KB5058403 (https://support.microsoft.com/en-in/help/5058403)
KB5058449 (https://support.microsoft.com/en-in/help/5058449)
KB5058392 (https://support.microsoft.com/en-in/help/5058392)
KB5058385 (https://support.microsoft.com/en-in/help/5058385)
KB5058497 (https://support.microsoft.com/en-in/help/5058497)
KB5058451 (https://support.microsoft.com/en-in/help/5058451)
KB5058454 (https://support.microsoft.com/en-in/help/5058454)
KB5058384 (https://support.microsoft.com/en-in/help/5058384)
KB5058500 (https://support.microsoft.com/en-in/help/5058500)
KB5058411 (https://support.microsoft.com/en-in/help/5058411)
KB5058383 (https://support.microsoft.com/en-in/help/5058383)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5058429 (https://support.microsoft.com/en-in/help/5058429)

KB5058430 (https://support.microsoft.com/en-in/help/5058430)

KB5058403 (https://support.microsoft.com/en-in/help/5058403)

KB5058449 (https://support.microsoft.com/en-in/help/5058449)

KB5058392 (https://support.microsoft.com/en-in/help/5058392)

KB5058385 (https://support.microsoft.com/en-in/help/5058385)

KB5058497 (https://support.microsoft.com/en-in/help/5058497)

KB5058451 (https://support.microsoft.com/en-in/help/5058451)

KB5058454 (https://support.microsoft.com/en-in/help/5058454)

KB5058384 (https://support.microsoft.com/en-in/help/5058384)

KB5058500 (https://support.microsoft.com/en-in/help/5058500)

KB5058411 (https://support.microsoft.com/en-in/help/5058411)

KB5058383 (https://support.microsoft.com/en-in/help/5058383)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

exploitdb
- Reference: CVE-2025-30397
- Description: Microsoft Windows Server 2025 JScript Engine - Remote Code Execution (RCE)
- Link: https://www.exploit-db.com/exploits/52315

github-exploits
- Reference: CVE-2025-30397
- Description: mbanyamer/CVE-2025-30397---Windows-Server-2025-JScript-RCE-Use-After-Free- exploit repository
- Link: https://github.com/mbanyamer/CVE-2025-30397---Windows-Server-2025-JScript-RCE-Use-After-Free-

blogs
- Reference: CVE-2025-30397
- Description: Microsoft Windows Server 2025 JScript Engine - Remote Code Execution (RCE)
- Link: https://www.exploit-db.com/raw/52315

nist-nvd2
- Reference: CVE-2025-30397
- Description: Access of resource using incompatible type ('type confusion') in Microsoft Scripting Engine allows an unauthorized attacker to execute code over a network.
- Link: https://www.vicarius.io/vsociety/posts/cve-2025-30397-type-confusion-vulnerability-in-microsoft-scripting-engine-detection-script

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5058392 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.17763.6292

4 Microsoft Windows Server Security Update for April 2025 CVSS: 4.5 CVSS3.1: 8.2 New

QID:	92235	CVSS Base:	5.4 [1]
Category:	Windows	CVSS Temporal:	4.5
Associated CVEs:	CVE-2025-27481, CVE-2025-27477, CVE-2025-21221, CVE-2025-21205, CVE-2025-21222, CVE-2025-27740, CVE-2025-26669, CVE-2025-27737, CVE-2025-26678, CVE-2025-27480, CVE-2025-27482, CVE-2025-26671, CVE-2025-26670, CVE-2025-26647, CVE-2025-26663, CVE-2025-27487, CVE-2025-29811, CVE-2025-27739, CVE-2025-24062, CVE-2025-24060, CVE-2025-27490, CVE-2025-27730, CVE-2025-27727, CVE-2025-27467, CVE-2025-27731, CVE-2025-29812, CVE-2025-27483, CVE-2025-26679, CVE-2025-24073, CVE-2025-26666, CVE-2025-27728, CVE-2025-26648, CVE-2025-27733, CVE-2025-27729, CVE-2025-26675, CVE-2025-26674, CVE-2025-26639, CVE-2025-24058, CVE-2025-21204, CVE-2025-24074, CVE-2025-29824, CVE-2025-27741, CVE-2025-27476, CVE-2025-26688, CVE-2025-27484, CVE-2025-27485, CVE-2025-29810, CVE-2025-27473, CVE-2025-26687, CVE-2025-26668, CVE-2025-27486, CVE-2025-27469, CVE-2025-26673, CVE-2025-26652, CVE-2025-26641, CVE-2025-21174, CVE-2025-27479, CVE-2025-27470, CVE-2025-26686, CVE-2025-26680, CVE-2025-29809, CVE-2025-27491, CVE-2025-27732, CVE-2025-27492, CVE-2025-26640, CVE-2025-26649, CVE-2025-21191, CVE-2025-27478, CVE-2025-27475, CVE-2025-26665, CVE-2025-26637, CVE-2025-26681, CVE-2025-27738, CVE-2025-26676, CVE-2025-26672, CVE-2025-26651, CVE-2025-26635, CVE-2025-21203, CVE-2025-21197, CVE-2025-27474, CVE-2025-26667, CVE-2025-26664, CVE-2025-27735, CVE-2025-27471, CVE-2025-27736, CVE-2025-27742, CVE-2025-26644, CVE-2025-29808, CVE-2025-27472, CVE-2024-21302		
Vendor Reference:	KB5055519, KB5055521, KB5055523, KB5055557, KB5055609, KB5055527, KB5055561, KB5055526, KB5055596, KB5055570, KB5055581		
Bugtraq ID:	-		
Service Modified:	05/20/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	8.2
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft Windows Server Security Update for April 2025

KB5055557 (https://support.microsoft.com/en-in/help/5055557)
KB5055609 (https://support.microsoft.com/en-in/help/5055609)
KB5055527 (https://support.microsoft.com/en-in/help/5055527)
KB5055521 (https://support.microsoft.com/en-in/help/5055521)
KB5055561 (https://support.microsoft.com/en-in/help/5055561)
KB5055526 (https://support.microsoft.com/en-in/help/5055526)
KB5055596 (https://support.microsoft.com/en-in/help/5055596)
KB5055519 (https://support.microsoft.com/en-in/help/5055519)
KB5055570 (https://support.microsoft.com/en-in/help/5055570)
KB5055581 (https://support.microsoft.com/en-in/help/5055581)
KB5055523 (https://support.microsoft.com/en-in/help/5055523)

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or may affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to refer following articles for more information on the vulnerabilities and patches.
KB5055557 (https://support.microsoft.com/en-in/help/5055557)
KB5055609 (https://support.microsoft.com/en-in/help/5055609)
KB5055527 (https://support.microsoft.com/en-in/help/5055527)
KB5055521 (https://support.microsoft.com/en-in/help/5055521)
KB5055561 (https://support.microsoft.com/en-in/help/5055561)
KB5055526 (https://support.microsoft.com/en-in/help/5055526)
KB5055596 (https://support.microsoft.com/en-in/help/5055596)
KB5055519 (https://support.microsoft.com/en-in/help/5055519)
KB5055570 (https://support.microsoft.com/en-in/help/5055570)
KB5055581 (https://support.microsoft.com/en-in/help/5055581)
KB5055523 (https://support.microsoft.com/en-in/help/5055523)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5055557 (https://support.microsoft.com/en-in/help/5055557)

KB5055609 (https://support.microsoft.com/en-in/help/5055609)

KB5055527 (https://support.microsoft.com/en-in/help/5055527)

KB5055521 (https://support.microsoft.com/en-in/help/5055521)

KB5055561 (https://support.microsoft.com/en-in/help/5055561)

KB5055526 (https://support.microsoft.com/en-in/help/5055526)

KB5055596 (https://support.microsoft.com/en-in/help/5055596)

KB5055519 (https://support.microsoft.com/en-in/help/5055519)

KB5055570 (https://support.microsoft.com/en-in/help/5055570)

KB5055581 (https://support.microsoft.com/en-in/help/5055581)

KB5055523 (https://support.microsoft.com/en-in/help/5055523)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

? github-exploits

Reference: CVE-2025-29824
Description: encrypter15/CVE-2025-29824 exploit repository
Link: https://github.com/encrypter15/CVE-2025-29824

? blogs

Reference: CVE-2024-21302
Description: Windows Downdate: Downgrade Attacks Using Windows Updates
Link: https://www.safebreach.com/blog/downgrade-attacks-using-windows-updates/

Reference: CVE-2024-21302
Description: An Update on Windows Downdate
Link: https://www.safebreach.com/blog/update-on-windows-downdate-downgrade-attacks/

Reference: CVE-2024-21302
Description: Windows Downdate: Downgrade Attacks Using Windows Updates
Link:
https://media.defcon.org/DEF%20CON%2032/DEF%20CON%2032%20presentations/DEF%20CON%2032%20-%20Alon%20Leviev

Reference: CVE-2025-21204
Description: Abusing the Windows Update Stack to Gain SYSTEM Access (CVE-2025-21204)
Link: https://cyberdom.blog/abusing-the-windows-update-stack-to-gain-system-access-cve-2025-21204/

Reference: CVE-2025-29824
Description: Ransomware Attackers Leveraged Privilege Escalation Zero-day
Link: https://www.security.com/threat-intelligence/play-ransomware-zero-day

nist-nvd2

Reference: CVE-2025-29824
Description: Use after free in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.
Link: https://www.vicarius.io/vsociety/posts/cve-2025-29824-windows-common-log-file-system-driver-elevation-of-privilege-vulnerability-det

Reference: CVE-2025-29824
Description: Use after free in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.
Link: https://www.vicarius.io/vsociety/posts/cve-2025-29824-windows-common-log-file-system-driver-elevation-of-privilege-vulnerability-miti

ASSOCIATED MALWARE:

Qualys Cloud Threat DB

Malware ID: Unattributed
Type: Ransomware
Link: https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/

Malware ID: RansomEXX
Type: Ransomware
Link: https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/

Malware ID: Play
Type: Ransomware
Link: https://www.security.com/threat-intelligence/play-ransomware-zero-day

RESULTS:

KB5055519 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.17763.6292

4 Microsoft Windows Server Security Update for February 2025 CVSS: 4.2 CVSS3.1: 7.9 New

QID:	92213	CVSS Base:	5.4 [1]
Category:	Windows	CVSS Temporal:	4.3
Associated CVEs:	CVE-2025-21351, CVE-2025-21352, CVE-2025-21368, CVE-2025-21369, CVE-2025-21375, CVE-2025-21376, CVE-2025-21379, CVE-2025-21182, CVE-2025-21183, CVE-2025-21391, CVE-2025-21418, CVE-2025-21419, CVE-2025-21420, CVE-2025-21208, CVE-2025-21406, CVE-2025-21407, CVE-2025-21410, CVE-2025-21190, CVE-2025-21200, CVE-2025-21201, CVE-2025-21337, CVE-2025-21347, CVE-2025-21349, CVE-2025-21350, CVE-2025-21358, CVE-2025-21359, CVE-2025-21367, CVE-2025-21371, CVE-2025-21377, CVE-2025-21179, CVE-2025-21181, CVE-2025-21184, CVE-2025-21212, CVE-2025-21216, CVE-2025-21254, CVE-2025-21414, CVE-2025-21373		
Vendor Reference:	KB5052016, KB5051979, KB5051980, KB5052000, KB5052072, KB5052032, KB5052020, KB5052042, KB5052006, KB5052038, KB5051987, KB5052105, KB5052106		
Bugtraq ID:	-		
Service Modified:	06/14/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group: -
Collateral Damage Potential: -
Target Distribution: -

Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

Microsoft Windows Server Security Update for February 2025

Affected Operating System: Windows Server 2008, Windows Server 2022, Windows Server 2019, Windows Server 2012, Windows Server 2016, Windows Server 2025

KB5052016 (https://support.microsoft.com/en-in/help/5052016)
KB5051979 (https://support.microsoft.com/en-in/help/5051979)
KB5051980 (https://support.microsoft.com/en-in/help/5051980)
KB5052000 (https://support.microsoft.com/en-in/help/5052000)
KB5052072 (https://support.microsoft.com/en-in/help/5052072)
KB5052032 (https://support.microsoft.com/en-in/help/5052032)
KB5052020 (https://support.microsoft.com/en-in/help/5052020)
KB5052042 (https://support.microsoft.com/en-in/help/5052042)
KB5052006 (https://support.microsoft.com/en-in/help/5052006)
KB5052038 (https://support.microsoft.com/en-in/help/5052038)
KB5051987 (https://support.microsoft.com/en-in/help/5051987)
KB5052105 (https://support.microsoft.com/en-in/help/5052105)
KB5052106 (https://support.microsoft.com/en-in/help/5052106)

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or may affect integrity, availability, and confidentiality.

SOLUTION:

Please refer to the following KB Articles associated with the update:KB5052016 (https://support.microsoft.com/en-in/help/5052016)
KB5051979 (https://support.microsoft.com/en-in/help/5051979)
KB5051980 (https://support.microsoft.com/en-in/help/5051980)
KB5052000 (https://support.microsoft.com/en-in/help/5052000)
KB5052072 (https://support.microsoft.com/en-in/help/5052072)
KB5052032 (https://support.microsoft.com/en-in/help/5052032)
KB5052020 (https://support.microsoft.com/en-in/help/5052020)
KB5052042 (https://support.microsoft.com/en-in/help/5052042)
KB5052006 (https://support.microsoft.com/en-in/help/5052006)
KB5052038 (https://support.microsoft.com/en-in/help/5052038)
KB5051987 (https://support.microsoft.com/en-in/help/5051987)
KB5052105 (https://support.microsoft.com/en-in/help/5052105)
KB5052106 (https://support.microsoft.com/en-in/help/5052106)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5052016 (https://support.microsoft.com/en-in/help/5052016)

KB5051979 (https://support.microsoft.com/en-in/help/5051979)

KB5051980 (https://support.microsoft.com/en-in/help/5051980)

KB5052000 (https://support.microsoft.com/en-in/help/5052000)

KB5052072 (https://support.microsoft.com/en-in/help/5052072)

KB5052032 (https://support.microsoft.com/en-in/help/5052032)

KB5052020 (https://support.microsoft.com/en-in/help/5052020)

KB5052042 (https://support.microsoft.com/en-in/help/5052042)

KB5052006 (https://support.microsoft.com/en-in/help/5052006)

KB5052038 (https://support.microsoft.com/en-in/help/5052038)

KB5051987 (https://support.microsoft.com/en-in/help/5051987)

KB5052105 (https://support.microsoft.com/en-in/help/5052105)

KB5052106 (https://support.microsoft.com/en-in/help/5052106)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
github-exploits
Reference: CVE-2025-21420

Description: Network-Sec/CVE-2025-21420-PoC exploit repository
Link: https://github.com/Network-Sec/CVE-2025-21420-PoC

Reference: CVE-2025-21420
Description: toxy4ny/edge-maradeur exploit repository
Link: https://github.com/toxy4ny/edge-maradeur

Reference: CVE-2025-21420
Description: moiz-2x/CVE-2025-21420_POC exploit repository
Link: https://github.com/moiz-2x/CVE-2025-21420_POC

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5052000 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.17763.6292

4 Microsoft Windows Server Security Update for December 2024 CVSS: 8.3 CVSS3.1: 9.1 New

QID:	92199	CVSS Base:	10.0[1]
Category:	Windows	CVSS Temporal:	8.3
Associated CVEs:	CVE-2024-49138, CVE-2024-49116, CVE-2024-49110, CVE-2024-49088, CVE-2024-49077, CVE-2024-49125, CVE-2024-49124, CVE-2024-49121, CVE-2024-49108, CVE-2024-49102, CVE-2024-49091, CVE-2024-49089, CVE-2024-49084, CVE-2024-49128, CVE-2024-49127, CVE-2024-49118, CVE-2024-49114, CVE-2024-49113, CVE-2024-49112, CVE-2024-49109, CVE-2024-49095, CVE-2024-49090, CVE-2024-49083, CVE-2024-49082, CVE-2024-49081, CVE-2024-49080, CVE-2024-49079, CVE-2024-49078, CVE-2024-49076, CVE-2024-49075, CVE-2024-49072, CVE-2024-49132, CVE-2024-49129, CVE-2024-49126, CVE-2024-49123, CVE-2024-49122, CVE-2024-49120, CVE-2024-49119, CVE-2024-49117, CVE-2024-49115, CVE-2024-49111, CVE-2024-49107, CVE-2024-49106, CVE-2024-49104, CVE-2024-49103, CVE-2024-49101, CVE-2024-49099, CVE-2024-49098, CVE-2024-49097, CVE-2024-49096, CVE-2024-49094, CVE-2024-49092, CVE-2024-49087, CVE-2024-49086, CVE-2024-49085, CVE-2024-49073, CVE-2024-49093, CVE-2024-38033		
Vendor Reference:	KB5048654, KB5048653, KB5048735, KB5048699, KB5048695, KB5048676, KB5048710, KB5048744, KB5048661, KB5048671		
Bugtraq ID:	-		
Service Modified:	06/19/2025	CVSS3.1 Base:	9.8
User Modified:	-	CVSS3.1 Temporal:	9.1
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft Windows Security Update - December 2024

KB5048654 (https://support.microsoft.com/en-in/help/5048654)
KB5048653 (https://support.microsoft.com/en-in/help/5048653)

KB5048735 (https://support.microsoft.com/en-in/help/5048735)
KB5048699 (https://support.microsoft.com/en-in/help/5048735)
KB5048695 (https://support.microsoft.com/en-in/help/5048695)
KB5048676 (https://support.microsoft.com/en-in/help/5048676)
KB5048710 (https://support.microsoft.com/en-in/help/5048710)
KB5048744 (https://support.microsoft.com/en-in/help/5048744)
KB5048671 (https://support.microsoft.com/en-in/help/5048671)
KB5048661 (https://support.microsoft.com/en-in/help/5048661)

IMPACT:

Successful exploit could compromise Confidentiality, Integrity and Availability

SOLUTION:

Please refer to the following KB Articles associated with the update:

KB5048654 (https://support.microsoft.com/en-in/help/5048654)
KB5048653 (https://support.microsoft.com/en-in/help/5048653)
KB5048735 (https://support.microsoft.com/en-in/help/5048735)
KB5048699 (https://support.microsoft.com/en-in/help/5048735)
KB5048695 (https://support.microsoft.com/en-in/help/5048695)
KB5048676 (https://support.microsoft.com/en-in/help/5048676)
KB5048710 (https://support.microsoft.com/en-in/help/5048710)
KB5048744 (https://support.microsoft.com/en-in/help/5048744)
KB5048671 (https://support.microsoft.com/en-in/help/5048671)
KB5048661 (https://support.microsoft.com/en-in/help/5048661)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5048654 (https://support.microsoft.com/en-in/help/5048654)

KB5048653 (https://support.microsoft.com/en-in/help/5048653)

KB5048735 (https://support.microsoft.com/en-in/help/5048735)

KB5048699 (https://support.microsoft.com/en-in/help/5048699)

KB5048695 (https://support.microsoft.com/en-in/help/5048695)

KB5048676 (https://support.microsoft.com/en-in/help/5048676)

KB5048710 (https://support.microsoft.com/en-in/help/5048710)

KB5048744 (https://support.microsoft.com/en-in/help/5048744)

KB5048671 (https://support.microsoft.com/en-in/help/5048671)

KB5048661 (https://support.microsoft.com/en-in/help/5048661)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

exploitdb

Reference: CVE-2024-49138
Description: Microsoft Windows 11 23h2 - CLFS.sys Elevation of Privilege
Link: https://www.exploit-db.com/exploits/52270

github-exploits

Reference: CVE-2024-49112
Description: SafeBreach-Labs/CVE-2024-49112 exploit repository
Link: https://github.com/SafeBreach-Labs/CVE-2024-49112

Reference: CVE-2024-49112
Description: CCIEVoice2009/CVE-2024-49112 exploit repository
Link: https://github.com/CCIEVoice2009/CVE-2024-49112

Reference: CVE-2024-49113
Description: SafeBreach-Labs/CVE-2024-49113 exploit repository
Link: https://github.com/SafeBreach-Labs/CVE-2024-49113

Reference: CVE-2024-49138
Description: MrAle98/CVE-2024-49138-POC exploit repository

Link: https://github.com/MrAle98/CVE-2024-49138-POC

Reference: CVE-2024-49138
Description: bananoname/CVE-2024-49138-POC exploit repository
Link: https://github.com/bananoname/CVE-2024-49138-POC

Reference: CVE-2024-49113
Description: 0xMetr0/metasploit-ldapnightmare exploit repository
Link: https://github.com/0xMetr0/metasploit-ldapnightmare

coreimpact
Reference: CVE-2024-49138
Description: Windows Common Log File System Driver LoadContainerQ Elevation of Privilege Vulnerability Exploit
Link: https://www.coresecurity.com/core-labs/exploits

blogs
Reference: CVE-2024-49113
Description: LDAPNightmare: SafeBreach Labs Publishes First Proof-of-Concept Exploit for CVE-2024-49113
Link: https://www.safebreach.com/blog/ldapnightmare-safebreach-labs-publishes-first-proof-of-concept-exploit-for-cve-2024-49113/

Reference: CVE-2024-49112
Description: LDAPNightmare: SafeBreach Labs Publishes First Proof-of-Concept Exploit for CVE-2024-49112
Link: https://www.safebreach.com/blog/ldapnightmare-safebreach-labs-publishes-first-proof-of-concept-exploit-for-cve-2024-49112/

Reference: CVE-2024-49113
Description: Windows LDAP Denial of Service Vulnerability (CVE-2024-49113): Crucial Information and How to Stay Protected
Link: https://www.sonicwall.com/blog/windows-ldap-dos-vulnerability-cve-2024-49113-what-you-need-to-know-and-tips-for-staying-protecte

Reference: CVE-2024-49138
Description: CVE-2024-49138 Windows CLFS heap-based buffer overflow analysis - Part 1
Link: https://security.humanativaspa.it/cve-2024-49138-windows-clfs-heap-based-buffer-overflow-analysis-part-1/

Reference: CVE-2024-49138
Description: CVE-2024-49138 Windows CLFS heap-based buffer overflow analysis - Part 2
Link: https://security.humanativaspa.it/cve-2024-49138-windows-clfs-heap-based-buffer-overflow-analysis-part-2/

Reference: CVE-2024-49138
Description: [One line a day] CVE-2024-49138: Windows Common Log File System Driver Elevation of Privilege Vulnerability
Link: https://hackyboiz.github.io/2025/06/18/ogu123/cve-2024-49138/

nist-nvd2
Reference: CVE-2024-49138
Description: Windows Common Log File System Driver Elevation of Privilege Vulnerability
Link: https://packetstorm.news/files/id/190585/

ASSOCIATED MALWARE:
ReversingLabs
Malware ID: CVE-2024-49138
Type: Exploit
Platform: Win64

Malware ID: Doina
Type: Trojan
Platform: Win64

RESULTS:

KB5048661 is not installed

%windir%\system32\ntoskrnl.exe Version is 10.0.17763.6292

4 Microsoft .NET Framework Security Update for June 2023 CVSS: 5.6 CVSS3.1: 6.8 New

QID:	92022	CVSS Base:	7.6 [1]
Category:	Windows	CVSS Temporal:	5.6
Associated CVEs:	CVE-2023-32030, CVE-2023-29326, CVE-2023-24895, CVE-2023-24936, CVE-2023-29331, CVE-2023-24897		
Vendor Reference:	KB5027544, KB5027536, KB5027123, KB5027540, KB5027531, KB5027542, KB5027533, KB5027541, KB5027532, KB5027543, KB5027534, KB5027219, KB5027230, KB5027538, KB5027119, KB5027537, KB5027539		
Bugtraq ID:	-		
Service Modified:	11/08/2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

A Denial of Service and Remote Code Execution Vulnerability exist in Microsoft .Net Framework.

Following KBs are covered in this detection:
KB5027540
KB5027531
KB5027542
KB5027533
KB5027541
KB5027532
KB5027543
KB5027534
KB5027219
KB5027230
KB5027538
KB5027119
KB5027537
KB5027539
KB5027544
KB5027536
KB5027123

This security update is rated Important for supported versions of Microsoft .NET Framework.

.NET Framework 2.0, 3.0, 3.5, 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, and 4.8.1

IMPACT:

Successful exploitation may allow a attacker to perform Denial of Service, Remote Code Execution and/or Elevation of Privileges.

SOLUTION:

Customers are advised to refer to CVE-2023-32030 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32030), CVE-2023-29326 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29326), CVE-2023-24895 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24895), CVE-2023-24936 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24936), CVE-2023-29331

(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29331), and CVE-2023-24897 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24897) for more details pertaining to these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2023-32030 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32030)

CVE-2023-29326 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29326)

CVE-2023-24895 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24895)

CVE-2023-24936 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24936)

CVE-2023-29331 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29331)

CVE-2023-24897 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24897)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5027536 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\Mscorlib.dll Version is 4.8.4110.0
%windir%\Microsoft.NET\Framework\v4.0.30319\Mscorlib.dll Version is 4.8.4110.0

4 Microsoft .NET Framework Denial of Service Vulnerability - February 2021 CVSS: 3.7 CVSS3.1: 6.5 New

QID:	91733	CVSS Base:	5.0
Category:	Windows	CVSS Temporal:	3.7
Associated CVEs:	CVE-2021-24111		
Vendor Reference:	KB4603005, KB4578951, KB4602958, KB4603002, KB4602960, KB4603004, KB4601051, KB4601056, KB4601318, KB4601354, KB4602961, KB4602959, KB4603003, KB4601050, KB4601054, KB4601887		
Bugtraq ID:	-		
Service Modified:	02/10/2021	CVSS3.1 Base:	7.5
User Modified:	-	CVSS3.1 Temporal:	6.5
Edited:	No		
PCI Vuln:	No		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

A denial of service vulnerability exist in Microsoft .Net Framework.

Following KBs are covered in this detection:
KB4601056, KB4601318, KB4601354, KB4601887, KB4602958, KB4602959, KB4602960, KB4602961, KB4603002, KB4603003, KB4603004
This security update is rated Important for supported versions of Microsoft .NET Framework.

.NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 and 4.8

IMPACT:

Successful exploitation allows attacker to cause denial of service vulnerability.

SOLUTION:

Customers are advised to refer to CVE-2021-24111 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24111) for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2021-24111 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24111)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB4601055 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\System.web.dll Version is 4.8.4110.0
%windir%\Microsoft.NET\Framework\v4.0.30319\System.web.dll Version is 4.8.4110.0

4 Microsoft .NET Framework Security Updates for October 2020 CVSS: 3.2 CVSS3.1: 4.1 New

QID:	91682	CVSS Base:	4.3
Category:	Windows	CVSS Temporal:	3.2
Associated CVEs:	CVE-2020-16937		
Vendor Reference:	KB4578968, KB4578969, KB4578971, KB4578972, KB4578974, KB4579976, KB4579977, KB4579978, KB4579979, KB4579980, KB4580327, KB4580328, KB4580330, KB4580467, KB4580468, KB4580469, KB4580470		
Bugtraq ID:	-		
Service Modified:	01/01/2024	CVSS3.1 Base:	4.7
User Modified:	-	CVSS3.1 Temporal:	4.1
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

An information disclosure vulnerability exists when the .NET Framework improperly handles objects in memory.

KB4578968,KB4578969,KB4578971,KB4578972,KB4578974,KB4579976,KB4579977,KB4579978,KB4579979,KB4579980,KB4580327,KB4580328,KB4580330,KB4580467,KB4580468,KB4580469,KB4580470 kbs are covered.

This security update is rated Important for supported versions of Microsoft .NET Framework.

.NET Framework 2.0, 3.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 and 4.8

IMPACT:

An attacker who successfully exploited the vulnerability can disclose contents of an affected system's memory.

SOLUTION:

Customers are advised to refer to CVE-2020-16937 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16937) for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2020-16937 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16937)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB4578973 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\System.security.dll Version is 4.8.3761.0
%windir%\Microsoft.NET\Framework\v4.0.30319\System.security.dll Version is 4.8.3761.0

4 Microsoft .NET Framework Security Updates for May 2020 CVSS: 4.1 CVSS3.1: 7.2 New

QID:	91634	CVSS Base:	5.0
Category:	Windows	CVSS Temporal:	4.1
Associated CVEs:	CVE-2020-1066, CVE-2020-1108		
Vendor Reference:	KB4552926, KB4552928, KB4552929, KB4552931, KB4556399, KB4556400, KB4556401, KB4556402, KB4556403, KB4556404, KB4556405, KB4556406, KB4556441, KB4556807, KB4556812, KB4556826		
Bugtraq ID:	-		
Service Modified:	05/30/2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	7.2
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

A denial of service vulnerability exists when .NET Framework improperly handles web requests.
An elevation of privilege vulnerability exists in .NET Framework which could allow an attacker to elevate their privilege level.

KB4552926,KB4552928,KB4552929,KB4552931,KB4556399,KB4556400,KB4556401,KB4556402,KB4556403,KB4556404,KB4556405,KB4556406,KB4556441,KB4556807,KB4556812,KB4556826 kbs are covered.
This security update is rated Important for supported versions of Microsoft .NET Framework.

IMPACT:

Successful exploitation allows attacker to elevate their privilege level and also cause a denial of service.

SOLUTION:

Customers are advised to refer to CVE-2020-1066 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1066), CVE-2020-1108 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1108) for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2020-1108 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1108)

CVE-2020-1066 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1066)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference:	CVE-2020-1066
Description:	Microsoft .NET Framework Local Privilege Escalation Exploit - Core Security Category : Exploits/Local

github-exploits

Reference:	CVE-2020-1066
Description:	cbwang505/CVE-2020-1066-EXP exploit repository
Link:	https://github.com/cbwang505/CVE-2020-1066-EXP

Reference:	CVE-2020-1066
Description:	Ascotbe/Kernelhub exploit repository
Link:	https://github.com/Ascotbe/Kernelhub

coreimpact

Reference:	CVE-2020-1066
Description:	Microsoft .NET Framework Elevation of Privilege Vulnerability Exploit
Link:	https://www.coresecurity.com/core-labs/exploits

gitee-exploits

Reference:	CVE-2020-1066
Description:	cbwang505/CVE-2020-1066-EXP exploit repository
Link:	https://gitee.com/cbwang505/CVE-2020-1066-EXP

ASSOCIATED MALWARE:

ReversingLabs

Malware ID:	CVE-2020-1066
Type:	Exploit
Platform:	Win32

Malware ID:	CVE-2017-0213
Type:	Exploit
Platform:	Win32

RESULTS:

KB4552930 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\Mscorlib.dll Version is 4.8.4110.0
%windir%\Microsoft.NET\Framework\v4.0.30319\Mscorlib.dll Version is 4.8.4110.0

4 Microsoft .NET Framework And .NET Core Security Updates for July 2020 CVSS: 5.3 CVSS3.1: 7 New

QID:	91658	CVSS Base:	6.8
Category:	Windows	CVSS Temporal:	5.3
Associated CVEs:	CVE-2020-1147		

Vendor Reference:	KB4565489, KB4565508, KB4565627, KB4565628, KB4565630, KB4565631, KB4565633, KB4566466, KB4566467, KB4566468, KB4566469, KB4566516, KB4566517, KB4566518, KB4566519, KB4566520, .NET Core July 2020		
Bugtraq ID:	-		
Service Modified:	04/09/2025	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	7.0
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

A remote code execution vulnerability exists in .NET Framework and .NET Core when the software fails to check the source markup of XML file input.

KB4565489,KB4565508,KB4565627,KB4565628,KB4565630,KB4565631,KB4565633,KB4566466,KB4566467,KB4566468,KB4566469,KB4566516,KB4566517,KB4566518,KB4566519,KB4566520 kbs and .Net Core are covered.
This security update is rated Critical for supported versions of Microsoft .NET Framework and .NET Core.

.NET Framework 2.0, 3.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 and 4.8
Any .NET Core 2.1 application running on .NET Core 2.1.19 or lower
.Any .NET Core 3.1 application running on .NET Core 3.1.5 or lower
Any .NET 5 application running on .NET 5 Preview 6 or lower

IMPACT:

An attacker who successfully exploited the vulnerability can run arbitrary code in the context of the process responsible for deserialization of the XML content.

SOLUTION:

Customers are advised to refer to CVE-2020-1147 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1147) for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2020-1147 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1147)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Core Security

Reference: CVE-2020-1147
Description: Microsoft SharePoint Server DataSet Deserialization Remote OS Command Injection Exploit (CVE-2020-1147) - Core Security Category : Exploits/OS Command Injection/Known Vulnerabilities

Metasploit

Reference: CVE-2020-1147
Description: SharePoint DataSet / DataTable Deserialization - Metasploit Ref : /modules/exploit/windows/http/sharepoint_data_deserialization
Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/http/sharepoint_data_deserialization.rb

The Exploit-DB

Reference: CVE-2020-1147
Description: Microsoft SharePoint Server 2019 - Remote Code Execution - The Exploit-DB Ref : 48747
Link: http://www.exploit-db.com/exploits/48747

Reference: CVE-2020-1147
Description: Microsoft SharePoint Server 2019 - Remote Code Execution (2) - The Exploit-DB Ref : 50151
Link: http://www.exploit-db.com/exploits/50151

exploitdb

Reference: CVE-2020-1147
Description: Microsoft SharePoint Server 2019 - Remote Code Execution (2)
Link: https://www.exploit-db.com/exploits/50151

Reference: CVE-2020-1147
Description: Microsoft SharePoint Server 2019 - Remote Code Execution
Link: https://www.exploit-db.com/exploits/48747

nvd

Reference: CVE-2020-1147
Description: A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'.
Link: http://packetstormsecurity.com/files/158694/SharePoint-DataSet-DataTable-Deserialization.html

Reference: CVE-2020-1147
Description: A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'.
Link: http://packetstormsecurity.com/files/158876/Microsoft-SharePoint-Server-2019-Remote-Code-Execution.html

Reference: CVE-2020-1147
Description: A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'.
Link: http://packetstormsecurity.com/files/163644/Microsoft-SharePoint-Server-2019-Remote-Code-Execution.html

Reference: CVE-2020-1147
Description: A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'.
Link: https://www.exploitalert.com/view-details.html?id=35992

packetstorm

Reference: CVE-2020-1147
Description: Microsoft SharePoint Server 2019 Remote Code Execution
Link: https://packetstormsecurity.com/files/158876/Microsoft-SharePoint-Server-2019-Remote-Code-Execution.html

Reference: CVE-2020-1147
Description: Microsoft SharePoint Server 2019 Remote Code Execution
Link: https://packetstormsecurity.com/files/163644/Microsoft-SharePoint-Server-2019-Remote-Code-Execution.html

Reference: CVE-2020-1147
Description: SharePoint DataSet / DataTable Deserialization
Link: https://packetstormsecurity.com/files/158694/SharePoint-DataSet-DataTable-Deserialization.html

metasploit

Reference: CVE-2020-1147
Description: SharePoint DataSet / DataTable Deserialization
Link: https://github.com/rapid7/metasploit-framework

Reference: CVE-2020-1147
Description: SharePoint DataSet / DataTable Deserialization
Link:
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/http/sharepoint_data_deserializatio

0day.today

Reference: CVE-2020-1147
Description: Microsoft SharePoint Server 2019 - Remote Code Execution Exploit (2)
Link: https://0day.today/exploit/36588

Reference: CVE-2020-1147
Description: Microsoft SharePoint Server 2019 - Remote Code Execution Exploit
Link: https://0day.today/exploit/34840

Reference: CVE-2020-1147
Description: SharePoint DataSet / DataTable Deserialization Exploit
Link: https://0day.today/exploit/34772

coreimpact

Reference: CVE-2020-1147
Description: Microsoft SharePoint Server DataSet Deserialization Remote OS Command Injection Exploit (CVE-2020-1147)
Link: https://www.coresecurity.com/core-labs/exploits

cisa-kev

Reference: CVE-2020-1147
Description: Microsoft .NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability
Link: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

gist

Reference: CVE-2020-1147
Description: SharePoint Authenticated (Low Privileged) RCE Exploit
Link: https://gist.github.com/0xcrypto/900b0ace57840f79ba2437850df7b81c

blogs

Reference: CVE-2020-1147
Description: Microsoft SharePoint Remote Code Execution Vulnerability (CVE-2020-1147)
Link: https://threatprotect.qualys.com/2020/07/24/microsoft-sharepoint-remote-code-execution-vulnerability-cve-2020-1147/

Reference: CVE-2020-1147
Description: SharePoint and Pwn :: Remote Code Execution Against SharePoint Server Abusing DataSet
Link: https://srcincite.io/blog/2020/07/20/sharepoint-and-pwn-remote-code-execution-against-sharepoint-server-abusing-dataset.html

nist-nvd2

Reference: CVE-2020-1147
Description: A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'.
Link: http://packetstormsecurity.com/files/158694/SharePoint-DataSet-DataTable-Deserialization.html

Reference: CVE-2020-1147
Description: A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'.
Link: https://www.exploitalert.com/view-details.html?id=35992

Reference: CVE-2020-1147
Description: A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'.
Link: http://packetstormsecurity.com/files/158876/Microsoft-SharePoint-Server-2019-Remote-Code-Execution.html

Reference: CVE-2020-1147
Description: A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'.
Link: http://packetstormsecurity.com/files/163644/Microsoft-SharePoint-Server-2019-Remote-Code-Execution.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB4565632 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\System.Data.dll Version is 4.8.3761.0
%windir%\Microsoft.NET\Framework\v4.0.30319\System.Data.dll Version is 4.8.3761.0

4 Microsoft .NET Framework Remote Code Execution Vulnerability for December 2022 CVSS: 5.5 CVSS3.1: 6.8 New

QID:	91961	CVSS Base:	7.5 [1]
Category:	Windows	CVSS Temporal:	5.5
Associated CVEs:	CVE-2022-41089		
Vendor Reference:	KB5021243, KB5021086, KB5021087, KB5020880, KB5021088, KB5021089, KB5021094, KB5021082, KB5020868, KB5021081, KB5021093, KB5021091, KB5021079, KB5021092, KB5021080, KB5021090, KB5021095, KB5020873, KB5021085		
Bugtraq ID:	-		
Service Modified:	12/02/2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

A Remote Code Execution Vulnerability exist in Microsoft .Net Framework.

Following KBs are covered in this detection:
KB5021243
KB5021086
KB5021087
KB5020880
KB5021088
KB5021089
KB5021094
KB5021082
KB5020868
KB5021081
KB5021093
KB5021091
KB5021079
KB5021092
KB5021080
KB5021090
KB5021095
KB5020873
KB5021085

This security update is rated Important for supported versions of Microsoft .NET Framework.

.NET Framework 2.0, 3.0, 3.5, 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, and 4.8.1

IMPACT:

Successful exploitation allows a attacker to cause Remote Code Execution Vulnerability.

SOLUTION:

Customers are advised to refer to CVE-2022-41089 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41089) for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2022-41089 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41089)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5021085 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\System.core.dll Version is 4.8.4110.0
%windir%\Microsoft.NET\Framework\v4.0.30319\System.core.dll Version is 4.8.4110.0

4 Microsoft SQL Server Remote Code Execution (RCE) Vulnerability for February 2023 CVSS: 4.4 CVSS3.1: 7.7 New

QID:	91983	CVSS Base:	6.0 [1]
Category:	Windows	CVSS Temporal:	4.4
Associated CVEs:	CVE-2023-21713, CVE-2023-21528, CVE-2023-21568, CVE-2023-21718, CVE-2023-21705, CVE-2023-21704, CVE-2023-23384		
Vendor Reference:	CVE-2023-21713, CVE-2023-21528, CVE-2023-21568, CVE-2023-21718, CVE-2023-21705, CVE-2023-21704		
Bugtraq ID:	-		
Service Modified:	09/23/2024	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft SQL Server prone to Remote Code Execution Vulnerability.

Affected Software:
SQL Server 2022 RTM (GDR)
SQL Server 2019 RTM

(GDR,CU18)
SQL Server 2017 RTM (GDR,CU31)
SQL Server 2016 Service Pack 3(GDR)
SQL Server 2014 Service Pack 3 (GDR, CU4)
SQL

Server 2008 R2 Service Pack 3 (GDR)

IMPACT:

Successful exploitation could lead to remote code execution

SOLUTION:

Customers are advised to refer to
KB5021522 (https://support.microsoft.com/help/5021522)
KB5021124 (https://support.microsoft.com/help/5021124)
KB5021126 (https://support.microsoft.com/help/5021126)
KB5021045 (https://support.microsoft.com/help/5021045)
KB5021127 (https://support.microsoft.com/help/5021127)
KB5021037 (https://support.microsoft.com/help/5021037)
KB5021129 (https://support.microsoft.com/help/5021129)
KB5021125 (https://support.microsoft.com/help/5021125)
KB5021128 (https://support.microsoft.com/help/5021128)
KB5021112 (https://support.microsoft.com/help/5021112)
for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

KB5021522 (https://support.microsoft.com/help/5021522)

KB5021126 (https://support.microsoft.com/help/5021126)

KB5021124 (https://support.microsoft.com/help/5021124)

KB5021045 (https://support.microsoft.com/help/5021045)

KB5021127 (https://support.microsoft.com/help/5021127)

KB5021037 (https://support.microsoft.com/help/5021037)

KB5021129 (https://support.microsoft.com/help/5021129)

KB5021125 (https://support.microsoft.com/help/5021125)

KB5021128 (https://support.microsoft.com/help/5021128)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

MSSQL 2022 Version is 2022.160.1000.6 Patch Version: 2022.160.1050.5

4 Microsoft .NET Framework Update for January 2024 CVSS: 6.3 CVSS3.1: 8.5 New

QID:	92097	CVSS Base:	8.5 [1]
Category:	Windows	CVSS Temporal:	6.3
Associated CVEs:	CVE-2024-0056, CVE-2024-21312, CVE-2024-0057, CVE-2023-36042		
Vendor Reference:	5034280, 5034270, 5033920, 5034272, 5034275, 5034274, 5034276, 5034279, 5034278, 5034269, 5034119, 5034273, 5034277, 5033910		
Bugtraq ID:	-		
Service Modified:	01/17/2024	CVSS3.1 Base:	9.8
User Modified:	-	CVSS3.1 Temporal:	8.5
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

A Denial of Service Vulnerability exist in Microsoft .Net Framework.

Following KBs are covered in this detection:
5034280
5034270
5033920
5034272
5034275
5034274
5034276
5034279
5034278
5034269
5034119
5034273
5034277
5033910

This security update is rated Important for supported versions of Microsoft .NET Framework.
.NET Framework 2.0, 3.0, 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, and 4.8.1

IMPACT:

Successful exploitation may allow a attacker to perform Denial of Service.

SOLUTION:

Customers are advised to refer to CVE-2024-0056 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0056), CVE-2024-21312 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312), CVE-2024-0057 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0057) for more details pertaining to these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-0056 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0056)

CVE-2024-21312 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312)

CVE-2024-0057 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0057)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5034273 is not installed
%windir%\Microsoft.NET\Framework64\v4.0.30319\System.dll Version is 4.8.4110.0
%windir%\Microsoft.NET\Framework\v4.0.30319\System.dll Version is 4.8.4110.0

4 Microsoft Visual C++ Redistributable Installer Elevation of Privilege Vulnerability CVSS: 5 CVSS3.1: 6.8 New

QID:	92183	CVSS Base:	6.8 [1]
Category:	Windows	CVSS Temporal:	5.0
Associated CVEs:	CVE-2024-43590		
Vendor Reference:	CVE-2024-43590		
Bugtraq ID:	-		
Service Modified:	11/18/2024	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

The Visual C++ Redistributable installs Microsoft C and C++ (MSVC) runtime libraries. Many applications built using Microsoft C and C++ tools require these libraries.

Affected Version:
The entire range of Visual C++ Redistributable installers from version 14.0 less than to 14.40.33810.0 is affected.

IMPACT:

An attacker who successfully exploited this vulnerability could create or delete files in the security context of the "NT AUTHORITY LOCAL SERVICE" account.

SOLUTION:

Customers are advised to update to latest version of Microsoft Visual C++ Redistributable. Refer to The Latest Supported Visual C++ Redistributable Downloads (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-43590) for more details.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-43590 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-43590)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HKLM\SOFTWARE\WOW6432Node\Microsoft\VisualStudio\14.0\VC\Runtimes\x64 Version = v14.36.32532.00
HKLM\SOFTWARE\WOW6432Node\Microsoft\VisualStudio\14.0\VC\Runtimes\x86 Version = v14.36.32532.00

4 Microsoft Windows Server Security Update for March 2025 CVSS: 5.5 CVSS3.1: 8.2 New

QID:	92226	CVSS Base:	6.7 [1]
Category:	Windows	CVSS Temporal:	5.5
Associated CVEs:	CVE-2025-26645, CVE-2025-26633, CVE-2025-24993, CVE-2025-24992, CVE-2025-24983, CVE-2025-24084, CVE-2025-24071, CVE-2025-24067, CVE-2025-24061, CVE-2025-24059, CVE-2025-24055, CVE-2025-24050, CVE-2025-24048, CVE-2025-24995, CVE-2025-21180, CVE-2025-24044, CVE-2025-24991, CVE-2025-24985, CVE-2025-24984, CVE-2025-24076, CVE-2025-24072, CVE-2025-24066, CVE-2025-24064, CVE-2025-24056, CVE-2025-24054, CVE-2025-24051, CVE-2025-24046, CVE-2025-24045, CVE-2025-21247, CVE-2025-25008, CVE-2025-24997, CVE-2025-24996, CVE-2025-24988, CVE-2025-24987, CVE-2024-9157, CVE-2025-24035		
Vendor Reference:	KB5053627, KB5053620, KB5053888, KB5053995, KB5053886, KB5053603, KB5053638, KB5053594, KB5053596, KB5053599, KB5053887, KB5053636		
Bugtraq ID:	-		
Service Modified:	06/15/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	8.2
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft Windows Server Security Update for March 2025

KB5053627 (https://support.microsoft.com/en-in/help/5053627)
KB5053620 (https://support.microsoft.com/en-in/help/5053620)
KB5053888 (https://support.microsoft.com/en-in/help/5053888)
KB5053995 (https://support.microsoft.com/en-in/help/5053995)
KB5053886 (https://support.microsoft.com/en-in/help/5053886)
KB5053603 (https://support.microsoft.com/en-in/help/5053603)
KB5053638 (https://support.microsoft.com/en-in/help/5053638)
KB5053594 (https://support.microsoft.com/en-in/help/5053594)
KB5053596 (https://support.microsoft.com/en-in/help/5053596)
KB5053599 (https://support.microsoft.com/en-in/help/5053599)
KB5053887 (https://support.microsoft.com/en-in/help/5053887)
KB5053636 (https://support.microsoft.com/en-in/help/5053636)

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or may affect integrity, availability, and confidentiality.

SOLUTION:

Please refer to the following KB Articles associated with the update:KB5053627 (https://support.microsoft.com/en-in/help/5053627)
KB5053620 (https://support.microsoft.com/en-in/help/5053620)
KB5053888 (https://support.microsoft.com/en-in/help/5053888)
KB5053995 (https://support.microsoft.com/en-in/help/5053995)
KB5053886 (https://support.microsoft.com/en-in/help/5053886)
KB5053603 (https://support.microsoft.com/en-in/help/5053603)
KB5053638 (https://support.microsoft.com/en-in/help/5053638)
KB5053594 (https://support.microsoft.com/en-in/help/5053594)
KB5053596 (https://support.microsoft.com/en-in/help/5053596)
KB5053599 (https://support.microsoft.com/en-in/help/5053599)
KB5053887 (https://support.microsoft.com/en-in/help/5053887)
KB5053636 (https://support.microsoft.com/en-in/help/5053636)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

KB5053627 (https://support.microsoft.com/en-in/help/5053627)

KB5053620 (https://support.microsoft.com/en-in/help/5053620)

KB5053888 (https://support.microsoft.com/en-in/help/5053888)

KB5053995 (https://support.microsoft.com/en-in/help/5053995)

KB5053886 (https://support.microsoft.com/en-in/help/5053886)

KB5053603 (https://support.microsoft.com/en-in/help/5053603)

KB5053638 (https://support.microsoft.com/en-in/help/5053638)

KB5053594 (https://support.microsoft.com/en-in/help/5053594)

KB5053596 (https://support.microsoft.com/en-in/help/5053596)

KB5053599 (https://support.microsoft.com/en-in/help/5053599)

KB5053887 (https://support.microsoft.com/en-in/help/5053887)

KB5053636 (https://support.microsoft.com/en-in/help/5053636)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

exploitdb

Reference: CVE-2025-24054
Description: Microsoft - NTLM Hash Disclosure Spoofing (library-ms)
Link: https://www.exploit-db.com/exploits/52280

Reference: CVE-2025-24071
Description: Windows File Explorer Windows 10 Pro x64 - TAR Extraction
Link: https://www.exploit-db.com/exploits/52325

Reference: CVE-2025-24071
Description: Windows File Explorer Windows 11 (23H2) - NTLM Hash Disclosure
Link: https://www.exploit-db.com/exploits/52310

Reference: CVE-2025-24076
Description: Microsoft Windows 11 Version 24H2 Cross Device Service - Elevation of Privilege
Link: https://www.exploit-db.com/exploits/52320

github-exploits

Reference: CVE-2025-24071
Description: FOLKS-iwd/CVE-2025-24071-msfvenom exploit repository
Link: https://github.com/FOLKS-iwd/CVE-2025-24071-msfvenom

Reference: CVE-2025-24071
Description: 0x6rss/CVE-2025-24071_PoC exploit repository
Link: https://github.com/0x6rss/CVE-2025-24071_PoC

Reference: CVE-2025-24071
Description: ctabango/CVE-2025-24071_PoCExtra exploit repository
Link: https://github.com/ctabango/CVE-2025-24071_PoCExtra

Reference: CVE-2025-24071
Description: cesarbtakeda/Windows-Explorer-CVE-2025-24071 exploit repository
Link: https://github.com/cesarbtakeda/Windows-Explorer-CVE-2025-24071

Reference: CVE-2025-24054
Description: xigney/CVE-2025-24054_PoC exploit repository
Link: https://github.com/xigney/CVE-2025-24054_PoC

Reference: CVE-2025-26633
Description: sandsoncosta/CVE-2025-26633 exploit repository
Link: https://github.com/sandsoncosta/CVE-2025-26633

Reference: CVE-2025-24071
Description: ThemeHackers/CVE-2025-24071 exploit repository
Link: https://github.com/ThemeHackers/CVE-2025-24071

Reference: CVE-2025-24071
Description: shacojx/CVE-2025-24071-Exploit exploit repository
Link: https://github.com/shacojx/CVE-2025-24071-Exploit

Reference: CVE-2025-24071
Description: rubbxalc/CVE-2025-24071 exploit repository
Link: https://github.com/rubbxalc/CVE-2025-24071

Reference: CVE-2025-24071
Description: Marcejr117/CVE-2025-24071_PoC exploit repository
Link: https://github.com/Marcejr117/CVE-2025-24071_PoC

Reference: CVE-2025-24054
Description: moften/CVE-2025-24054 exploit repository
Link: https://github.com/moften/CVE-2025-24054

Reference: CVE-2025-24071
Description: pswalia2u/CVE-2025-24071_POC exploit repository
Link: https://github.com/pswalia2u/CVE-2025-24071_POC

Reference: CVE-2025-24054
Description: helidem/CVE-2025-24054-PoC exploit repository
Link: https://github.com/helidem/CVE-2025-24054-PoC

Reference: CVE-2025-24071
Description: xigney/CVE-2025-24054_PoC exploit repository
Link: https://github.com/xigney/CVE-2025-24054_PoC

Reference: CVE-2025-24054
Description: S4mma3l/CVE-2025-24054 exploit repository
Link: https://github.com/S4mma3l/CVE-2025-24054

Reference: CVE-2025-24054
Description: ClementNjeru/CVE-2025-24054-PoC exploit repository
Link: https://github.com/ClementNjeru/CVE-2025-24054-PoC

Reference: CVE-2025-24054
Description: Yuri08loveElaina/CVE-2025-24054_POC exploit repository
Link: https://github.com/Yuri08loveElaina/CVE-2025-24054_POC

Reference: CVE-2025-24071
Description: f4dee-backup/CVE-2025-24071 exploit repository
Link: https://github.com/f4dee-backup/CVE-2025-24071

Reference: CVE-2025-24071
Description: LOOKY243/CVE-2025-24071-PoC exploit repository
Link: https://github.com/LOOKY243/CVE-2025-24071-PoC

Reference: CVE-2025-24076
Description: mbanyamer/CVE-2025-24076 exploit repository
Link: https://github.com/mbanyamer/CVE-2025-24076

Reference: CVE-2025-24071
Description: DeshanFer94/CVE-2025-24071-POC-NTLMHashDisclosure- exploit repository
Link: https://github.com/DeshanFer94/CVE-2025-24071-POC-NTLMHashDisclosure-

Reference: CVE-2025-24035
Description: MSeymenD/cve-2025-24035-rds-websocket-dos-test exploit repository

Link: https://github.com/MSeymenD/cve-2025-24035-rds-websocket-dos-test

Reference: CVE-2025-24071
Description: B1ack4sh/Blackash-CVE-2025-24071 exploit repository
Link: https://github.com/B1ack4sh/Blackash-CVE-2025-24071

Reference: CVE-2025-24071
Description: TH-SecForge/CVE-2025-24071 exploit repository
Link: https://github.com/TH-SecForge/CVE-2025-24071

Reference: CVE-2025-24071
Description: helidem/CVE-2025-24054_CVE-2025-24071-PoC exploit repository
Link: https://github.com/helidem/CVE-2025-24054_CVE-2025-24071-PoC

Reference: CVE-2025-24054
Description: helidem/CVE-2025-24054_CVE-2025-24071-PoC exploit repository
Link: https://github.com/helidem/CVE-2025-24054_CVE-2025-24071-PoC

Reference: CVE-2025-24071
Description: ex-cal1bur/SMB_CVE-2025-24071 exploit repository
Link: https://github.com/ex-cal1bur/SMB_CVE-2025-24071

coreimpact
Reference: CVE-2025-24054
Description: Microsoft Windows library-ms NTLMv2 Information Disclosure Exploit
Link: https://www.coresecurity.com/core-labs/exploits

blogs
Reference: CVE-2025-24071
Description: CVE-2025-24071: NTLM Hash Leak via RAR/ZIP Extraction and .library-ms File
Link: https://cti.monster/blog/2025/03/18/CVE-2025-24071.html

Reference: CVE-2025-26633
Description: CVE-2025-26633: How Water Gamayun Weaponizes MUIPath using MSC EvilTwin
Link: https://www.trendmicro.com/en_us/research/25/c/cve-2025-26633-water-gamayun.html

Reference: CVE-2025-24076
Description: 300 Milliseconds to Admin: Mastering DLL Hijacking and Hooking to Win the Race (CVE-2025-24076 and CVE-2025-24994)
Link:
https://blog.compass-security.com/2025/04/3-milliseconds-to-admin-mastering-dll-hijacking-and-hooking-to-win-the-race-cve-2025-24

Reference: CVE-2025-24071
Description: Windows File Explorer Windows 11 (23H2) - NTLM Hash Disclosure
Link: https://www.exploit-db.com/raw/52310

vulncheck-initial-access
Reference: CVE-2025-24054
Description: Windows 11 NTLMv2 Hash Leak
Link: https://api.vulncheck.com/v3/index/initial-access?cve=CVE-2025-24054

nist-nvd2
Reference: CVE-2025-26633
Description: Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally.
Link:
https://www.vicarius.io/vsociety/posts/cve-2025-26633-security-feature-bypass-in-microsoft-management-console-detection-script

Reference: CVE-2025-26633
Description: Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally.
Link:
https://www.vicarius.io/vsociety/posts/cve-2025-26633-security-feature-bypass-in-microsoft-management-console-mitigation-script

Reference: CVE-2025-24054

Description: External control of file name or path in Windows NTLM allows an unauthorized attacker to perform spoofing over a network.
Link:
https://www.vicarius.io/vsociety/posts/cve-2025-24054-spoofing-vulnerability-in-windows-ntlm-by-microsoft-detection-script

Reference: CVE-2025-24985
Description: Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally.
Link:
https://www.vicarius.io/vsociety/posts/cve-2025-24985-integer-overflow-vulnerability-in-microsoft-windows-fast-fat-driver-detection-scr

ASSOCIATED MALWARE:

ReversingLabs
Malware ID: CVE-2025-24054
Type: Exploit
Platform: Win32,Document

Qualys Cloud Threat DB
Malware ID: Larva-208
Type: Ransomware
Link: https://www.trendmicro.com/en_us/research/25/c/cve-2025-26633-water-gamayun.html

Malware ID: Unattributed
Type: Ransomware
Link: https://www.trendmicro.com/en_us/research/25/c/cve-2025-26633-water-gamayun.html

RESULTS:

KB5053596 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.17763.6292

4 Microsoft Windows DWM Core Library Elevation of Privilege Vulnerability for May 2025 CVSS: 3.6 CVSS3.1: 7.2 New

QID:	92264	CVSS Base:	4.3 [1]
Category:	Windows	CVSS Temporal:	3.6
Associated CVEs:	CVE-2025-30400		
Vendor Reference:	CVE-2025-30400		
Bugtraq ID:	-		
Service Modified:	05/14/2025	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	7.2
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft Windows DWM Core Library Elevation of Privilege Vulnerability CVE-2025-30400 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30400).

Affected Operating System: Windows 11 Version 22H2, Windows Server 2022 Core, Windows 10 Version 21H2, Windows 10 Version 1809, Windows 11 Version 24H2, Windows Server 2019 Core, Windows Server 23H2, Windows 10 Version 22H2, Windows Server 2022, Azure Stack HCI Version 22H2, Windows Server 2025, Windows 11 Version 23H2, Windows Server 2025 Core, Windows Server 2019

The KB Articles associated with the update:
Patch version is 10.0.26100.4061 for KB5058411 (https://support.microsoft.com/help/5058411).
Patch version is 10.0.25398.1611 for KB5058384 (https://support.microsoft.com/help/5058384).
Patch version is 10.0.22621.5331 for KB5058405 (https://support.microsoft.com/help/5058405).
Patch version is 10.0.19041.5848 for KB5058379 (https://support.microsoft.com/help/5058379).
Patch version is 10.0.20348.3692 for KB5058385 (https://support.microsoft.com/help/5058385).
Patch version is 10.0.17763.7309 for KB5058392 (https://support.microsoft.com/help/5058392).
Security Hotpatch update for Windows Server 2025 and Windows 11 Version 24H2 is KB5058497 (https://support.microsoft.com/help/5058497).
Security Hotpatch update for Windows Server 2022 is KB5058500 (https://support.microsoft.com/help/5058500).

IMPACT:

Successful exploitation of this vulnerability may allow an authorized attacker to elevate privileges locally.

SOLUTION:

Vendor has released patch. Please refer to the Microsoft Security Advisory (CVE-2025-30400) (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30400) for further information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2025-30400: WIndows (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30400)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5058392 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.17763.6292

4 Microsoft Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability for May 2025 CVSS: 3.6 CVSS3.1: 7.2 New

QID:	92265	CVSS Base:	4.3 [1]
Category:	Windows	CVSS Temporal:	3.6
Associated CVEs:	CVE-2025-32709		
Vendor Reference:	CVE-2025-32709		
Bugtraq ID:	-		
Service Modified:	05/15/2025	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	7.2
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-

Integrity Requirement: -
Availability Requirement: -

THREAT:

Microsoft Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability CVE-2025-32709 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32709).

Affected Operating System: Windows 11 Version 22H2, Windows Server 2022 Core, Windows Server 2016 Core, Windows 10 Version 21H2, Windows 10 Version 1507, Windows 10 Version 1809, Windows Server 2022, Azure Stack HCI Version 22H2, Windows Server 2016, Windows Server 2012 R2 Core, Windows Server 2025 Core, Windows Server 2012 Core, Windows Server 2019 Core, Windows 11 Version 23H2, Windows Server 2012 R2, Windows 11 Version 24H2, Windows 10 Version 1607, Windows Server 2019, Windows 10 Version 22H2, Windows Server 23H2, Windows Server 2025, Windows Server 2012

The KB Articles associated with the update:
KB5058383 (https://support.microsoft.com/en-in/help/5058383)
KB5058451 (https://support.microsoft.com/en-in/help/5058451)
KB5058379 (https://support.microsoft.com/en-in/help/5058379)
KB5058403 (https://support.microsoft.com/en-in/help/5058403)
KB5058384 (https://support.microsoft.com/en-in/help/5058384)
KB5058405 (https://support.microsoft.com/en-in/help/5058405)
KB5058392 (https://support.microsoft.com/en-in/help/5058392)
KB5058387 (https://support.microsoft.com/en-in/help/5058387)
KB5058385 (https://support.microsoft.com/en-in/help/5058385)
KB5058411 (https://support.microsoft.com/en-in/help/5058411)

IMPACT:

Successful exploitation of this vulnerability may allows an authorized attacker to elevate privileges locally.

SOLUTION:

Vendor has released patch. Please refer to the Microsoft Security Advisory (CVE-2025-32709) (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32709) for further information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2025-32709 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32709)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

KB5058392 is not installed
%windir%\system32\ntoskrnl.exe Version is 10.0.17763.6292

4 Microsoft SQL Server, ODBC and OLE DB Driver for SQL Server Multiple Vulnerabilities for October 2023 CVSS: 3.4 CVSS3.1: 6.8 New

QID:	378931	CVSS Base:	4.6 [1]
Category:	Local	CVSS Temporal:	3.4
Associated CVEs:	CVE-2023-36728, CVE-2023-36730, CVE-2023-36420, CVE-2023-36785, CVE-2023-36417		
Vendor Reference:	CVE-2023-36728, CVE-2023-36730, CVE-2023-36420, CVE-2023-36785, CVE-2023-36417		
Bugtraq ID:	-		
Service Modified:	04/25/2024	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft has released a security update to addressed a Remote Code Execution Vulnerability in OLE DB and ODBC driver for SQL Server. Both of these are APIs for Microsoft SQL server that provide access to a range of data sources.

Affected Software:
Microsoft ODBC Driver 17 for SQL Server on Windows version prior to 17.10.5.1
Microsoft ODBC Driver 18 for SQL Server on Windows version prior to 18.3.2.1
Microsoft ODBC Driver 17 for SQL Server on Linux version prior to 17.10.5.1
Microsoft ODBC Driver 18 for SQL Server on Linux version prior to 18.3.2.1
Microsoft SQL Server 2022 for x64-based Systems (GDR)
Microsoft SQL Server 2019 for x64-based Systems (GDR)
Microsoft SQL Server 2022 for x64-based Systems ((CU 8))
Microsoft SQL Server 2019 for x64-based Systems (CU 22)
Microsoft SQL Server 2017 for x64-based Systems (CU 31)
Microsoft SQL Server 2017 for x32-based Systems (CU 31)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU 4)
Microsoft SQL Server 2014 Service Pack 3 for x32-based Systems (GDR)
Microsoft OLE DB Driver 19 for SQL Server version prior to 19.3.2.0
Microsoft OLE DB Driver 18 for SQL Server version prior to 18.6.7.0

IMPACT:

Successful exploitation may lead to remote code execution and denial of service.

SOLUTION:

Customers are advised to refer to CVE-2023-36728 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36728), CVE-2023-36730 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36730), CVE-2023-36420 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36420), CVE-2023-36785 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36785), CVE-2023-36417 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36417), for more information regarding the vulnerabilities and their patches.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2023-36728 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36728)

CVE-2023-36730 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36730)

CVE-2023-36420 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36420)

CVE-2023-36785 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36785)

CVE-2023-36417 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36417)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

MSSQL 2022 Version is 2022.160.1000.6 Patch Version: 2022.160.1105.1

4 Multi-Remote Next Generation Connection Manager (mRemoteNG) Password Dumper Vulnerability CVSS: 9 CVSS3.1: 7.1 New

QID:	379270	CVSS Base:	10.0[1]
Category:	Local	CVSS Temporal:	9.0
Associated CVEs:	CVE-2023-30367		
Vendor Reference:	CVE-2023-30367		
Bugtraq ID:	-		
Service Modified:	01/29/2024	CVSS3.1 Base:	7.5
User Modified:	-	CVSS3.1 Temporal:	7.1
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Multi-Remote Next Generation Connection Manager (mRemoteNG) is free software that enables users to store and manage multi-protocol connection configurations to remotely connect to systems. mRemoteNG configuration files can be stored in an encrypted state on disk. mRemoteNG version less than v1.76.21 and less than 1.77.4-dev loads configuration files in plain text into memory (after decrypting them if necessary) at application start-up, even if no connection has been established yet.

Affected Version :
mRemoteNG version prior to v1.76.21

IMPACT:

It allows attackers to access contents of configuration files in plain text through a memory dump and thus compromise user credentials when no custom password encryption key has been set.

SOLUTION:

Update to mRemoteNG greater than v1.77.3.1784-NB when a fix has been released, please refer to advisory here.
(https://github.com/S1lkys/CVE-2023-30367-mRemoteNG-password-dumper).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm

Reference: CVE-2023-30367

Description: mRemoteNG 1.77.3.1784-NB Sensitive Information Extraction

Link:

https://packetstormsecurity.com/files/173829/mRemoteNG-1.77.3.1784-NB-Sensitive-Information-Extraction.html

0day.today

Reference: CVE-2023-30367
Description: mRemoteNG v1.77.3.1784-NB - Cleartext Storage of Sensitive Information in Memory Exploit
Link: https://0day.today/exploit/38917

github-exploits

Reference: CVE-2023-30367
Description: S1lkys/CVE-2023-30367-mRemoteNG-password-dumper exploit repository
Link: https://github.com/S1lkys/CVE-2023-30367-mRemoteNG-password-dumper

nist-nvd2

Reference: CVE-2023-30367
Description: Multi-Remote Next Generation Connection Manager (mRemoteNG) is free software that enables users to store and manage multi-protocol connection configurations to remotely connect to systems. mRemoteNG configuration files can be stored in an encrypted state on disk. mRemoteNG version
Link: http://packetstormsecurity.com/files/173829/mRemoteNG-1.77.3.1784-NB-Sensitive-Information-Extraction.html

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\mRemoteNG\mRemoteNG.exe Version is 1.76.20.24615

4 Microsoft SQL Server ODBC and OLE DB Driver for SQL Server Multiple Vulnerabilities for July 2024 CVSS: 3.4 CVSS3.1: 7.7 New

QID:	380160	CVSS Base:	4.6 [1]
Category:	Local	CVSS Temporal:	3.4
Associated CVEs:	CVE-2024-37320, CVE-2024-20701, CVE-2024-21317, CVE-2024-21331, CVE-2024-21425, CVE-2024-37319, CVE-2024-35272, CVE-2024-35271, CVE-2024-38087, CVE-2024-21303, CVE-2024-37321, CVE-2024-21428, CVE-2024-21415, CVE-2024-37324, CVE-2024-21449, CVE-2024-37326, CVE-2024-37327, CVE-2024-37328, CVE-2024-37329, CVE-2024-37330, CVE-2024-37334, CVE-2024-37333, CVE-2024-37336, CVE-2024-28928, CVE-2024-35256, CVE-2024-38088, CVE-2024-37322, CVE-2024-21332, CVE-2024-37323, CVE-2024-21335, CVE-2024-37318, CVE-2024-37332, CVE-2024-37331, CVE-2024-21414, CVE-2024-21333, CVE-2024-21398, CVE-2024-21373, CVE-2024-21308		
Vendor Reference:	CVE-2024-37320, CVE-2024-20701, CVE-2024-21317, CVE-2024-21331, CVE-2024-21425, CVE-2024-37319, CVE-2024-35272, CVE-2024-35271, CVE-2024-38087, CVE-2024-21303, CVE-2024-37321, CVE-2024-21428, CVE-2024-21415, CVE-2024-37324, CVE-2024-21449, CVE-2024-37326, CVE-2024-37327, CVE-2024-37328, CVE-2024-37329, CVE-2024-37330, CVE-2024-37334, CVE-2024-37333, CVE-2024-37336, CVE-2024-28928, CVE-2024-35256, CVE-2024-38088, CVE-2024-37322, CVE-2024-21332, CVE-2024-37323, CVE-2024-21335, CVE-2024-37318, CVE-2024-37332, CVE-2024-37331, CVE-2024-21414, CVE-2024-21333, CVE-2024-21398, CVE-2024-21373, CVE-2024-21308		
Bugtraq ID:	-		
Service Modified:	10/07/2024	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group: -
Collateral Damage Potential: -
Target Distribution: -

Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

Microsoft has released a security update to addressed a Remote Code Execution Vulnerability in OLE DB and ODBC driver for SQL Server. Both of these are APIs for Microsoft SQL server that provide access to a range of data sources.

Affected Software:
Microsoft SQL Server 2017 for x64-based Systems (CU 30)
Microsoft SQL Server 2019 for x64-based Systems (CU 26)
Microsoft SQL Server 2022 for x64-based Systems (CU 12)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR) Version 2015.130.6441.0 and below
Microsoft SQL Server 2017 for x64-based Systems (GDR) Version 2017.140.2056.1 and below
Microsoft SQL Server 2019 for x64-based Systems (GDR) Version 2019.150.2116.1 and below
Microsoft SQL Server 2022 for x64-based Systems (GDR) Version 2022.160.1121.3 and below
Microsoft OLE DB Driver 18 for SQL Server version prior to 18.7.0004.0 (18.7.4)
Microsoft OLE DB Driver 19 for SQL Server version prior to 19.3.0005.0 (19.3.5)

IMPACT:

Successful exploitation may lead to remote code execution.

SOLUTION:

Customers are advised to refer to CVE-2024-37320 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37320), CVE-2024-20701 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-20701), CVE-2024-21317 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21317), CVE-2024-21331 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21331), CVE-2024-21425 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21425), CVE-2024-37319 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37319), CVE-2024-35272 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-35272), CVE-2024-35271 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-35271), CVE-2024-38087 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38087), CVE-2024-21303 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21303), CVE-2024-37321 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37321), CVE-2024-21428 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21428), CVE-2024-21415 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21415), CVE-2024-37324 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37324), CVE-2024-21449 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21449), CVE-2024-37326 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37326), CVE-2024-37327 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37327), CVE-2024-37328 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37328), CVE-2024-37329 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37329), CVE-2024-37330 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37330), CVE-2024-37334 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37334), CVE-2024-37333 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37333), CVE-2024-37336 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37336), CVE-2024-28928 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-28928), CVE-2024-35256 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-35256), CVE-2024-38088 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38088), CVE-2024-37322 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37322), CVE-2024-21332 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21332) for more information regarding the vulnerabilities and their patches.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-37320 (https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37320)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

MSSQL 2022 Version is 2022.160.1000.6 Patch Version: 2022.160.1121.4

4 Microsoft SQL Server Multiple Vulnerabilities for September 2024 CVSS: 7.4 CVSS3.1: 8.5 New

QID:	380469	CVSS Base:	10.0[1]
Category:	Local	CVSS Temporal:	7.4
Associated CVEs:	CVE-2024-37341, CVE-2024-37980, CVE-2024-37965, CVE-2024-43474, CVE-2024-26191, CVE-2024-26186, CVE-2024-37342, CVE-2024-37337, CVE-2024-37339, CVE-2024-37340, CVE-2024-37335, CVE-2024-37966, CVE-2024-37338		
Vendor Reference:	CVE-2024-37341, CVE-2024-37980, CVE-2024-37965, CVE-2024-43474, CVE-2024-26191, CVE-2024-26186, CVE-2024-37342, CVE-2024-37337, CVE-2024-37339, CVE-2024-37340, CVE-2024-37335, CVE-2024-37966, CVE-2024-37338		
Bugtraq ID:	-		
Service Modified:	10/21/2024	CVSS3.1 Base:	9.8
User Modified:	-	CVSS3.1 Temporal:	8.5
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft has released a security update to address Remote code execution, Information disclosure, and Privilege escalation vulnerabilities in SQL Server.

Affected Software:
Microsoft SQL Server 2017 for x64-based Systems (CU 31)
Microsoft SQL Server 2019 for x64-based Systems (CU 28)
Microsoft SQL Server 2022 for x64-based Systems (CU 14)
Microsoft SQL Server 2016 Service Pack 3 Azure Connect Feature Pack
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)
Microsoft SQL Server 2017 for x64-based Systems (GDR)
Microsoft SQL Server 2019 for x64-based Systems (GDR)
Microsoft SQL Server 2022 for x64-based Systems (GDR)

IMPACT:

Successful exploitation may lead to Remote code execution, Information disclosure, and Privilege escalation vulnerability.

SOLUTION:

Refer to
CVE-2024-37341 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37341)
CVE-2024-37980 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37980)
CVE-2024-37965 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37965)
CVE-2024-43474 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43474)
CVE-2024-26191 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26191)
CVE-2024-26186 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26186)
CVE-2024-37342 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37342)
CVE-2024-37337 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37337)

CVE-2024-37339 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37339)
CVE-2024-37340 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37340)
CVE-2024-37335 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37335)
CVE-2024-37966 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37966)
CVE-2024-37338 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37338)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-37341 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37341)

CVE-2024-37980 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37980)

CVE-2024-37965 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37965)

CVE-2024-43474 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43474)

CVE-2024-26191 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26191)

CVE-2024-26186 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26186)

CVE-2024-37342 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37342)

CVE-2024-37337 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37337)

CVE-2024-37339 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37339)

CVE-2024-37340 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37340)

CVE-2024-37335 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37335)

CVE-2024-37966 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37966)

CVE-2024-37338 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37338)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

MSSQL 2022 Version is 2022.160.1000.6 Patch Version: 2022.160.1125.1

4 Microsoft SQL Server Multiple Vulnerabilities for November 2024 CVSS: 7.4 CVSS3.1: 7.7 New

QID:	382336	CVSS Base:	10.0[1]
Category:	Local	CVSS Temporal:	7.4
Associated CVEs:	CVE-2024-38255, CVE-2024-43459, CVE-2024-43462, CVE-2024-48993, CVE-2024-48994, CVE-2024-48995, CVE-2024-48996, CVE-2024-48997, CVE-2024-48998, CVE-2024-48999, CVE-2024-49000, CVE-2024-49001, CVE-2024-49002, CVE-2024-49003, CVE-2024-49004, CVE-2024-49005, CVE-2024-49006, CVE-2024-49007, CVE-2024-49008, CVE-2024-49009, CVE-2024-49010, CVE-2024-49011, CVE-2024-49012, CVE-2024-49013, CVE-2024-49014, CVE-2024-49015, CVE-2024-49016, CVE-2024-49017, CVE-2024-49018, CVE-2024-49021, CVE-2024-49043		
Vendor Reference:	CVE-2024-38255, CVE-2024-43459, CVE-2024-43462, CVE-2024-48993, CVE-2024-48994, CVE-2024-48995, CVE-2024-48996, CVE-2024-48997, CVE-2024-48998, CVE-2024-48999, CVE-2024-49000, CVE-2024-49001, CVE-2024-49002, CVE-2024-49003, CVE-2024-49004, CVE-2024-49005, CVE-2024-49006, CVE-2024-49007, CVE-2024-49008, CVE-2024-49009, CVE-2024-49010, CVE-2024-49011, CVE-2024-49012, CVE-2024-49013, CVE-2024-49014, CVE-2024-49015, CVE-2024-49016, CVE-2024-49017, CVE-2024-49018, CVE-2024-49021		
Bugtraq ID:	-		
Service Modified:	11/13/2024	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft has released a security update to address Remote code execution, Information disclosure, and Privilege escalation vulnerabilities in SQL Server.

Affected Software:
Microsoft SQL Server 2017 for x64-based Systems (CU 31)
Microsoft SQL Server 2019 for x64-based Systems (CU 29)
Microsoft SQL Server 2016 Service Pack 3 Azure Connect Feature Pack
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)
Microsoft SQL Server 2017 for x64-based Systems (GDR)
Microsoft SQL Server 2019 for x64-based Systems (GDR)
Microsoft SQL Server 2022 for x64-based Systems (GDR)

IMPACT:

Successful exploitation may lead to remote code execution vulnerability.

SOLUTION:

Refer to,
CVE-2024-38255 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38255)
CVE-2024-43459 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-43459)
CVE-2024-43462 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-43462)
CVE-2024-48993 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-48993)
CVE-2024-48994 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-48994)
CVE-2024-48995 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-48995)
CVE-2024-48996 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-48996)
CVE-2024-48997 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-48997)
CVE-2024-48998 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-48998)
CVE-2024-48999 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-48999)
CVE-2024-49000 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-49000)
CVE-2024-49001 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-49001)
CVE-2024-49002 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-49002)
CVE-2024-49003 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-49003)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2024-38255 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38255)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

MSSQL 2022 Version is 2022.160.1000.6 Patch Version: 2022.160.1135.2

 4 Microsoft Edge Based on Chromium Prior to 131.0.2903.48 Multiple Vulnerabilities CVSS: 4.2 CVSS3.1: 7.9 New

QID:	382361	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.3
Associated CVEs:	CVE-2024-11117, CVE-2024-11116, CVE-2024-11115, CVE-2024-11114, CVE-2024-11113, CVE-2024-11112, CVE-2024-11111, CVE-2024-11110, CVE-2024-49025		
Vendor Reference:	Edge (chromium based) 131.0.2903.48		
Bugtraq ID:	-		
Service Modified:	01/03/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 131.0.2903.48 or later (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#november-14-2024)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 131.0.2903.48 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#november-14-2024)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

nist-nvd2

Reference:	CVE-2024-11111
Description:	Inappropriate implementation in Autofill in Google Chrome prior to 131.0.6778.69 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)
Link:	https://issues.chromium.org/issues/360520331

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 131.0.2903.63 Multiple Vulnerabilities CVSS: 4 CVSS3.1: 7.7 New

QID:	382396	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2024-11395, CVE-2024-49054		

Vendor Reference:	Edge (chromium based) 131.0.2903.63		
Bugtraq ID:	-		
Service Modified:	11/25/2024	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 131.0.2903.63 or later (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#november-21-2024)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 131.0.2903.63 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#november-21-2024)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 131.0.2903.146 Multiple Vulnerabilities

CVSS: 7.4 CVSS3.1: 7.7 New

QID:	382677	CVSS Base:	10.0[1]
Category:	Local	CVSS Temporal:	7.4
Associated CVEs:	CVE-2025-0291		
Vendor Reference:	Edge (chromium based) 131.0.2903.146		
Bugtraq ID:	-		
Service Modified:	04/28/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 131.0.2903.146 or later
(https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#january-10-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 131.0.2903.146 (https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#january-10-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 132.0.2957.140 Multiple Vulnerabilities CVSS: 4 CVSS3.1: 7.7 New

QID:	382753	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-0762		
Vendor Reference:	Edge (chromium based) 132.0.2957.140		
Bugtraq ID:	-		
Service Modified:	02/03/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-

Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 132.0.2957.140 or later
(https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#january-30-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 132.0.2957.140 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#january-30-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 133.0.3065.51/Extended Stable 132.0.2957.171 Multiple Vulnerabilities CVSS: 4 CVSS3.1: 7.7 New

QID:	382796	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-21404, CVE-2025-21408, CVE-2025-21279, CVE-2025-21267, CVE-2025-21342, CVE-2025-21283		
Vendor Reference:	Edge (chromium based) 133.0.3065.51		
Bugtraq ID:	-		
Service Modified:	02/25/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:
Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 133.0.3065.51 or later/Extended Stable 132.0.2957.171 or later (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#february-6-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 133.0.3065.51 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#february-6-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 133.0.3065.92/Extended Stable 132.0.2957.178 Multiple Vulnerabilities

CVSS: 4 CVSS3.1: 7.7 New

QID:	382872	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-1006, CVE-2025-1426, CVE-2025-0999		
Vendor Reference:	Edge (chromium based) 133.0.3065.82		
Bugtraq ID:	-		
Service Modified:	03/17/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 133.0.3065.92 or later/Extended Stable 132.0.2957.178 or later (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#february-21-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 133.0.3065.82 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#february-21-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 134.0.3124.83 Multiple Vulnerabilities

CVSS: 4 CVSS3.1: 7.7 New

QID:	382970	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-2476		
Vendor Reference:	Edge (chromium based) 134.0.3124.83		
Bugtraq ID:	-		
Service Modified:	03/25/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 134.0.3124.83 or later (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#march-21-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 134.0.3124.83 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#march-21-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 134.0.3124.93 Multiple Vulnerabilities CVSS: 4.2 CVSS3.1: 7.5 New

QID:	382999	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.3
Associated CVEs:	CVE-2025-2783, CVE-2025-29834		
Vendor Reference:	Edge (chromium based) 134.0.3124.93		
Bugtraq ID:	-		
Service Modified:	05/31/2025	CVSS3.1 Base:	8.3
User Modified:	-	CVSS3.1 Temporal:	7.5
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 134.0.3124.93 or later
(https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#march-26-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 134.0.3124.93 (https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#march-26-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

blogs

Reference:	CVE-2025-2783
Description:	CVE-2025-2783 Deep Dive Analysis
Link:	https://blog.securelayer7.net/cve-2025-2783-chrome-mojo-ipc-sandbox/

Reference: CVE-2025-2783
Description: ChromSploit-Framework/exploits/cve_2025_2783.py
Link: https://github.com/Leviticus-Triage/ChromSploit-Framework/blob/main/exploits/cve_2025_2783.py

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 135.0.3179.54 Multiple Vulnerabilities CVSS: 5.6 CVSS3.1: 7.7 New

QID:	383043	CVSS Base:	7.6 [1]
Category:	Local	CVSS Temporal:	5.6
Associated CVEs:	CVE-2025-3066, CVE-2025-3067, CVE-2025-3068, CVE-2025-3069, CVE-2025-3070, CVE-2025-3071, CVE-2025-3072, CVE-2025-3073, CVE-2025-3074, CVE-2025-25000		
Vendor Reference:	Edge (chromium based) 135.0.3179.54		
Bugtraq ID:	-		
Service Modified:	04/28/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 135.0.3179.54 or later (https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#april-3-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 135.0.3179.54 (https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#april-3-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 136.0.3240.50 Multiple Vulnerabilities CVSS: 4.1 CVSS3.1: 8.5 New

QID:	383162	CVSS Base:	5.5 [1]
Category:	Local	CVSS Temporal:	4.1
Associated CVEs:	CVE-2025-4052, CVE-2025-4051, CVE-2025-4050, CVE-2025-4096, CVE-2025-29825		
Vendor Reference:	Edge (chromium based) 136.0.3240.50		
Bugtraq ID:	-		
Service Modified:	05/07/2025	CVSS3.1 Base:	9.8
User Modified:	-	CVSS3.1 Temporal:	8.5
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 136.0.3240.50 or later
(https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#may-1-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 136.0.3240.50 (https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#may-1-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 136.0.3240.64 Multiple Vulnerabilities CVSS: 4 CVSS3.1: 7.7 New

QID:	383200	CVSS Base:	5.4 [1]

Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-4372		
Vendor Reference:	Edge (chromium based) 136.0.3240.64		
Bugtraq ID:	-		
Service Modified:	05/12/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 136.0.3240.64 or later (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-4372)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 136.0.3240.64 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-4372)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

4 Microsoft Edge Based on Chromium Prior to 137.0.3296.62/Extended Stable 136.0.3240.115 Multiple Vulnerabilities

CVSS: 4 CVSS3.1: 7.7 New

QID:	383331	CVSS Base:	5.4 [1]
Category:	Local	CVSS Temporal:	4.0
Associated CVEs:	CVE-2025-5419, CVE-2025-5068		
Vendor Reference:	Edge (chromium based) 137.0.3296.62		
Bugtraq ID:	-		
Service Modified:	06/17/2025	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		

PCI Vuln: Yes
Ticket State:

First Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Last Detected: 06/26/2025 at 10:14:32 PM (GMT-0400)

Times Detected: 1

Last Fixed: N/A

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

EdgeChromium has released security update for Mac and Windows to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to version 137.0.3296.62 or later
(https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#june-3-2025)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Edge (chromium based) 137.0.3296.62 (https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#june-3-2025)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Version is 129.0.2792.65

Appendix

No results available for these hosts

10.159.10.108,172.31.1.2-172.31.1.50

No vulnerabilities match your filters for these hosts (50)

10.159.10.108, 172.31.1.2-172.31.1.50

Report Filters

Vulnerability Lists:	Scan Report Template: High Severity Report
Status:	New, Active, Re-Opened, Fixed
Display non-running kernels:	Off
Exclude non-running kernels:	Off
Exclude non-running services:	Off
Exclude QIDs not exploitable due to configuration:	Off
Vulnerabilities:	State:Active
Included Operating Systems:	All Operating Systems

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

Severity	Level	Description
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

Footnotes

This footnote indicates that the CVSS Base score that is displayed for the vulnerability is not supplied by NIST. When the service looked up the latest NIST score for the vulnerability, as published in the National Vulnerability Database (NVD), NIST either listed the CVSS Base score as 0 or did not provide a score in the NVD. In this case, the service determined that the severity of the vulnerability warranted a higher CVSS Base score. The score provided by the service is displayed.

This report was generated with an evaluation version of Qualys