Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Patch Tuesday Alert: 63 Fixes, 2 Zero-Days, and a Race Against Hackers

Date of Publication	Admiralty Code	TA Number
February 13, 2025	A1	TA2025040

Summary

First Seen: February 11, 2025
Affected Products: Microsoft SharePoint Server, Microsoft Office, Windows Win32K, Windows LDAP, Microsoft Excel, Microsoft Dynamics 365 Sales
Impact: Elevation of Privilege (EoP), Remote Code Execution (RCE), Spoofing, Feature Bypass

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-21377	NTLM Hash Disclosure Spoofing Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21391	Windows Storage Elevation of Privilege Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-21418	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-21194	Microsoft Surface Security Feature Bypass Vulnerability	Microsoft Surface	✗	✗	✓
CVE-2025-21184	Windows Core Messaging Elevation of Privileges Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21358	Windows Core Messaging Elevation of Privileges Vulnerability	Microsoft Windows	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-21400	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server	✗	✗	✓
CVE-2025-21414	Windows Core Messaging Elevation of Privileges Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21367	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21376	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21419	Windows Setup Files Cleanup Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21420	Windows Disk Cleanup Tool Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21379	DHCP Client Service Remote Code Execution Vulnerability	Windows DHCP Server	✗	✗	✓
CVE-2025-21381	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	✗	✗	✓
CVE-2025-21177	Microsoft Dynamics 365 Sales Elevation of Privilege Vulnerability	Microsoft Dynamics 365 Sales	✗	✗	✓

Vulnerability Details

#1

Microsoft's February 2025 Patch Tuesday delivers security updates for 67 vulnerabilities, including four critical and 56 important severity flaws. Among these, two zero-day vulnerabilities, which are actively exploited in real-world attacks, have been addressed, while two others were publicly disclosed before a fix was available.

#2

This month's patches address a range of security risks, including 25 Remote Code Execution (RCE) vulnerabilities, 20 Elevation of Privilege (EoP) flaws, two Security Feature Bypass issues, nine Denial of Service (DoS) vulnerabilities, five Spoofing flaws, and one Information Disclosure and Tampering vulnerability.

#3

One of the most pressing flaws is CVE-2025-21391, a Windows Storage Elevation of Privilege vulnerability. Microsoft has patched this actively exploited issue, which allows attackers to delete specific files on a system. While it does not grant access to sensitive information, it can be used to delete critical data, potentially disrupting services and making systems unavailable. Attackers with the right permissions could exploit this flaw to delete files essential for system stability, making it a significant security risk.

#4

Another serious threat is CVE-2025-21418, a vulnerability in the Windows Ancillary Function Driver for WinSock. This flaw allows attackers to escalate their privileges to the SYSTEM level, granting them full control over an affected machine. SYSTEM privileges provide the highest level of access in Windows, enabling attackers to execute code, modify system settings, and install malicious software. Since this vulnerability has already been exploited in attacks, applying Microsoft's latest patches is critical.

#5

Two additional publicly disclosed vulnerabilities before Microsoft issued fixes, increasing the risk of exploitation. CVE-2025-21194, a Microsoft Surface Security Feature Bypass vulnerability, exploits a hypervisor flaw, allowing attackers to bypass UEFI security and compromise the secure kernel.

#6

This is particularly concerning for virtual machines running on UEFI-based host machines, as attackers could gain control of the hypervisor and secure kernel, both critical for system protection. On specific hardware configurations, this flaw could be leveraged to override essential security measures, posing a significant risk.

#7

Another publicly disclosed vulnerability, CVE-2025-21377, presents a different but equally serious threat. This NTLM Hash Disclosure Spoofing vulnerability allows attackers to steal Windows users' NTLM authentication hashes, which could then be used to impersonate users and gain unauthorized access. The danger lies in its minimal user interaction requirement even single-click, right-click, or previewing a malicious file could trigger the flaw, exposing users to potential attacks without opening or executing the file.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-21184	Windows Versions 10 and 11 Windows Server 2016, 2019, 2022, 23H2 Edition (Server Core installation), 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2025-21358	Windows version 10, 11 Windows Server 2016, 2019, 2022, 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-822
CVE-2025-21367	Windows 10, 11 Windows Server 2019, 2022, 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-21376	Microsoft Windows 10, 11 Microsoft Windows Server 2008, 2012, 2016, 2019, 2022, 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122 CWE-191 CWE-362
CVE-2025-21377	Windows 10, 11 Windows Server 2008, 2012, 2016, 2019, 2022, 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-73
CVE-2025-21391	Windows 10, 11 Windows Server 2016, 2019, 2022, 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-59
CVE-2025-21400	Microsoft SharePoint Server: 2019 Microsoft SharePoint Server Subscription Edition: All versions Microsoft SharePoint Enterprise Server: 2016	cpe:2.3:a:microsoft:microsoft_sharepoint_server:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_sharepoint_server_subscription_edition:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_sharepoint_enterprise_server:-:*:*:*:*:*:*:*	CWE-285
CVE-2025-21414	Windows 10, 11 Windows Server 2016, 2019, 2022, 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2025-21418	Windows Server 2008, 2012, 2016, 2019, 2022, 2025 Windows 10, 11	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-21419	Windows Server 2008, 2012, 2016, 2019, 2022, 2025 Windows 10, 11	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-59
CVE-2025-21420	Windows Server 2012, 2016, 2019, 2022, 2025 Windows 10, 11	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-59
CVE-2025-21194	Microsoft Surface	cpe:2.3:o:microsoft:surface:-:*:*:*:*:*:*:*	CWE-20
CVE-2025-21379	Windows Server: before 2016 10.0.14393.7785, 2025 10.0.26100.3107, 2025 10.0.26100.3194, 2016 10.0.14393.7785	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-21381	Office Online Server: All versions Microsoft Office: 2019 Microsoft Excel: 2016 Microsoft Office LTSC: 2021 for Mac - 2024 Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	cpe:2.3:a:microsoft:office_online_server:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_office_ltsc:-:forMac:*:*:*:*:*:*	CWE-822
CVE-2025-21177	Microsoft Dynamics 365 Sales customer relationship management (CRM) software	cpe:2.3:a:microsoft:dynamics_365_sales:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:dynamics_365:*:*:*:*:*:*:*:*	CWE-918

Recommendations

Keep your systems up to date by implementing the most recent security updates. To avoid the introduction of new vulnerabilities, follow security rules adapted to unique devices. Furthermore, to strengthen the resilience of devices and apps exposed to the internet, thoroughly review their configurations.

Conduct an extensive service exposure evaluation to identify any vulnerable services that may be publicly accessible. Take immediate and decisive action to address any identified vulnerabilities, either by installing essential **patches** or adopting other security measures.

Exercise meticulous surveillance on any security-related events that occur within devices and applications. If any abnormalities are discovered, take prompt action to begin the incident management procedure.

Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0042** Resource Development
TA0040 Impact	**T1203** Exploitation for Client Execution	**T1059** Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1588.005** Exploits	**T1040** Network Sniffing
T1498 Network Denial of Service	**T1204** User Execution	**T1133** External Remote Services	**T1562** Impair Defenses
T1190 Exploit Public-Facing Application	**T1553** Subvert Trust Controls	**T1485** Data Destruction	**T1498** Network Denial of Service

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21184

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21358

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21367

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21376

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21377

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21391

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21400

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21414

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21418

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21419

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21420

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21194

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21379

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21381

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21177

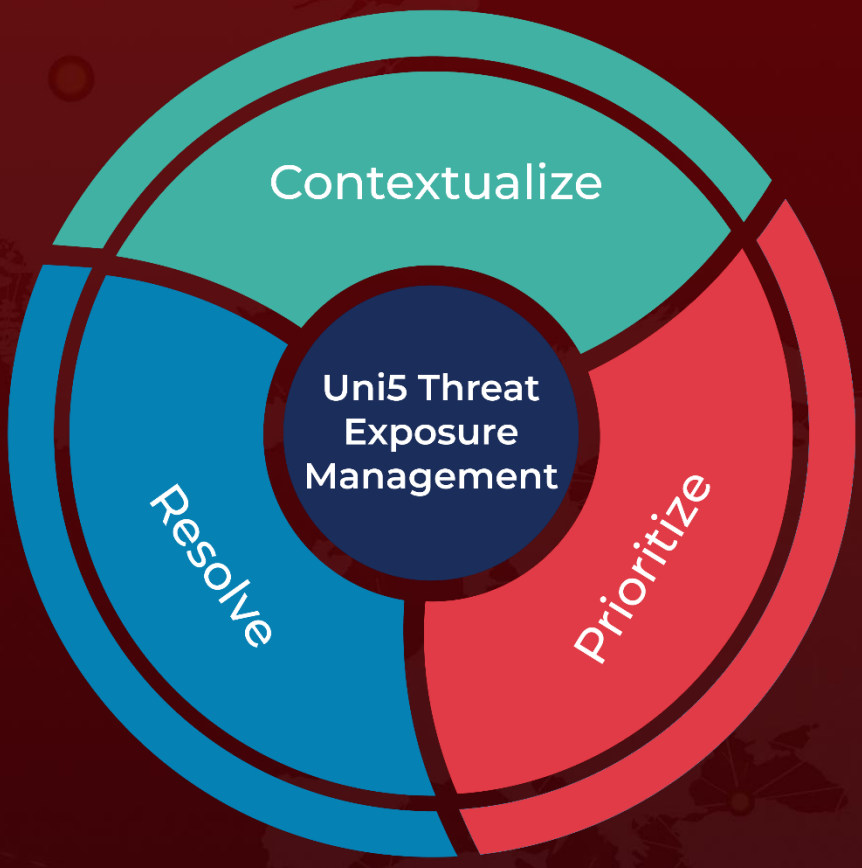
References

https://msrc.microsoft.com/update-guide/releaseNote/2025-Feb

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 13, 2025 • 9:00 PM

More at www.hivepro.com