

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Microsoft's January 2025 Patch Tuesday Fixes Active Zero-Day Exploits

Date of Publication

January 20, 2025

Admiralty Code

A1

TA Number

TA2025012
















Summary

First Seen: January 14, 2025

Affected Platforms: Microsoft Windows, Microsoft Office SharePoint, Microsoft Office, Windows Kerberos, Windows Kernel, Windows Remote Desktop Services, Windows Secure Boot, and more.

Impact: Denial of Service (DoS), Elevation of Privilege (EoP), Remote Code Execution (RCE), Information Disclosure, Security Feature Bypass and Spoofing.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-21333	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2025-21334	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2025-21335	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2025-21366	Microsoft Access Remote Code Execution Vulnerability	Microsoft Access			
CVE-2025-21395	Microsoft Access Remote Code Execution Vulnerability	Microsoft Access			

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-21186	Microsoft Access Remote Code Execution Vulnerability	Microsoft Access	✗	✗	✓
CVE-2025-21275	Windows App Package Installer Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21308	Windows Themes Spoofing Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21297	Windows Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21309	Windows Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-21298	Windows OLE Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓

Vulnerability Details

#1

Microsoft's January 2025 Patch Tuesday includes security updates for 162 vulnerabilities, classified as 12 critical, 149 important, and 1 moderate-severity vulnerability. These encompass 58 Remote Code Execution, 43 Elevation of Privilege, 22 Information Disclosure, 20 Denial of Service, 14 Security Feature Bypass, and 5 Spoofing vulnerabilities. The updates apply to a broad range of Microsoft products, including Windows, Office, Windows Remote Desktop Services, Windows Hyper-V, Microsoft Office SharePoint, Azure Marketplace SaaS Resources, and other components.

#2

Notably, Microsoft also patched sixteen non-Microsoft vulnerabilities. This includes one assigned to Windows by CERT CC, one assigned to Visual Studio by GitHub, and fourteen affecting the Chromium-based Microsoft Edge browser, bringing the total number of CVEs to 178. This advisory addresses 11 CVEs with potential exploitation risks.

#3

The update resolves three zero-day vulnerabilities that are actively being exploited in the wild and five that have been publicly disclosed. This extensive patch cycle aims to address critical issues and enhance overall system security.

#4

Among the actively exploited zero-day vulnerabilities are CVE-2025-21333, CVE-2025-21334, and CVE-2025-21335, all of which are elevation of privilege vulnerabilities in Windows Hyper-V NT Kernel Integration VSP. These flaws could allow an authenticated local attacker to gain SYSTEM privileges. All three were being exploited in the wild before patches were made available, highlighting the urgency for users to apply the updates immediately.

#5

In addition to the actively exploited flaws, Microsoft also addressed five vulnerabilities that had been publicly disclosed prior to patches. These include CVE-2025-21186, CVE-2025-21366, and CVE-2025-21395, all of which are remote code execution vulnerabilities in Microsoft Access. Exploiting these vulnerabilities requires an attacker to trick a user into opening a malicious file, potentially leading to arbitrary code execution.

#6

Similarly, CVE-2025-21308, a spoofing vulnerability in Windows Themes, and CVE-2025-21275, an elevation of privilege vulnerability in the Windows App Package Installer, were publicly disclosed and remain critical concerns.

#7

The update also addressed several critical vulnerabilities that, while not zero-days, pose significant risks. Notable among these are CVE-2025-21297 and CVE-2025-21309, remote code execution vulnerabilities in Windows Remote Desktop Services. These flaws could allow attackers to execute arbitrary code by exploiting a race condition within the Remote Desktop Gateway role. Another critical vulnerability, CVE-2025-21298, affects Windows OLE and could enable remote code execution through a specially crafted email opened in a vulnerable version of Microsoft Outlook.

#8

Given the severity of these vulnerabilities, especially those that are actively exploited or publicly disclosed, organizations and individual users are strongly encouraged to apply the latest patches without delay to protect their systems from potential exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-21333	Windows: 10 - 11 24H2 Windows Server: 2022 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-122
CVE-2025-21334	Windows: 10 - 11 24H2 Windows Server 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-416
CVE-2025-21335	Windows: 10 - 11 24H2 Windows Server 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-416
CVE-2025-21366	Microsoft Office 2019 Microsoft Access 2016 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:office:*:*:*:*:*:* cpe:2.3:a:microsoft:access:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*	CWE-416
CVE-2025-21395	Microsoft Office 2019 Microsoft Access 2016 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:office:*:*:*:*:*:* cpe:2.3:a:microsoft:access:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*	CWE-122
CVE-2025-21186	Microsoft Office 2019 Microsoft Access 2016 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:office:*:*:*:*:*:* cpe:2.3:a:microsoft:access:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*	CWE-122
CVE-2025-21275	Windows: 10 - 11 24H2 Windows Server : 2022 & 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-285

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-21308	Windows: 10 - 11 24H2 Windows Server: 2012 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-200
CVE-2025-21297	Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-416
CVE-2025-21309	Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-591
CVE-2025-21298	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-416

Recommendations



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 security measures.



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.



Prioritize patching the actively exploited vulnerabilities CVE-2025-21333, CVE-2025-21334, and CVE-2025-21335. These vulnerabilities pose significant exploitation risks and should be addressed urgently.



Implement network segmentation to restrict unauthorized access and reduce the impact of potential attacks. This can be especially effective in scenarios where network adjacency is a factor.



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

<u>TA0004</u> Privilege Escalation	<u>TA0042</u> Resource Development	<u>TA0040</u> Impact	<u>TA0002</u> Execution
<u>TA0008</u> Lateral Movement	<u>TA0001</u> Initial Access	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits
<u>T1059</u> Command and Scripting Interpreter	<u>T1588.006</u> Vulnerabilities	<u>T1068</u> Exploitation for Privilege Escalation	<u>T1203</u> Exploitation for Client Execution
<u>T1498</u> Network Denial of Service	<u>T1566</u> Phishing	<u>T1204</u> User Execution	<u>T1210</u> Exploitation of Remote Services
<u>T1133</u> External Remote Services			

Patch Links

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21334>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21366>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21395>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21186>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21275>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21308>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21297>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21309>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21298>

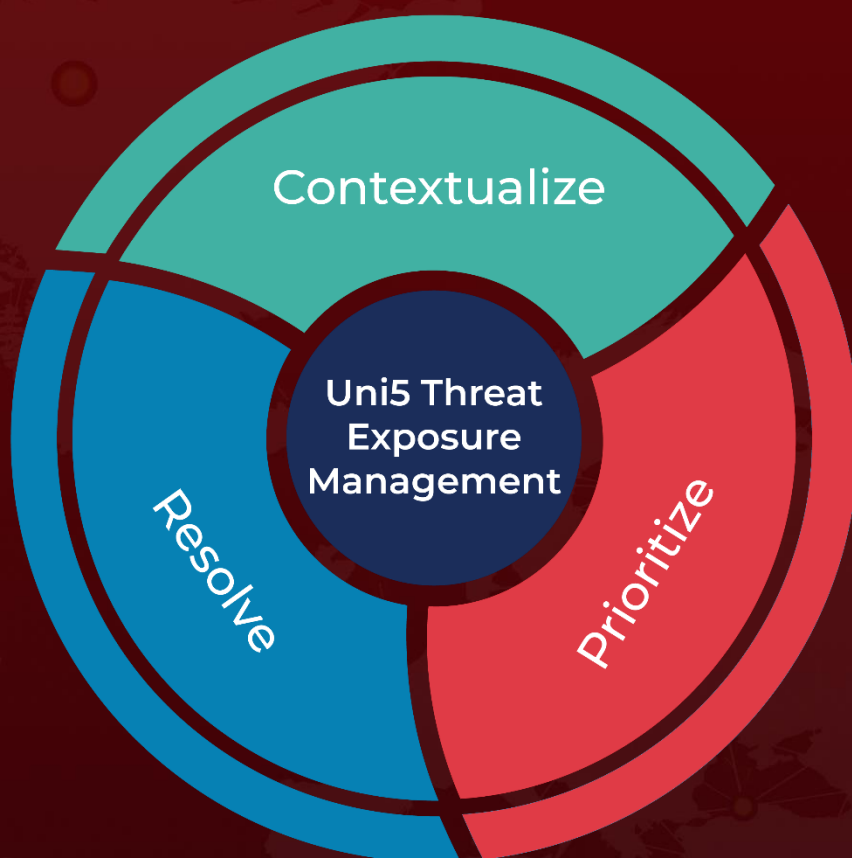
References

<https://msrc.microsoft.com/update-guide/releaseNote/2025-Jan>

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

January 20, 2025 • 7:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com