Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's September Patch Tuesday Addresses Active Zero-Day Exploits

Date of Publication	Last updated date	Admiralty Code	TA Number
September 12, 2024	September 16, 2024	A1	TA2024352

Summary

First Seen: September 10, 2024
Affected Platforms: Microsoft Windows, Microsoft SharePoint Server, Microsoft Office, Microsoft Azure, Microsoft Outlook
Impact: Elevation of Privilege (EoP), Remote Code Execution (RCE), Information Disclosure, Denial of Service (DoS), Security Feature Bypass, and Spoofing

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-38014	Windows Installer Elevation of Privilege Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-38217	Windows Mark of the Web Security Feature Bypass Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-38226	Microsoft Publisher Security Feature Bypass Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-43491	Microsoft Windows Update Remote Code Execution Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-38018	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-38227	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server	✗	✗	✓
CVE-2024-38228	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server	✗	✗	✓
CVE-2024-38237	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38238	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38241	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38242	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38243	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38244	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38245	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-38246	Win32k Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38247	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38249	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38252	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38253	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-43457	Windows Setup and Deployment Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-43461	Windows MSHTML Platform Spoofing Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2024-43464	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server	✗	✗	✓
CVE-2024-43487	Windows Mark of the Web Security Feature Bypass Vulnerability	Microsoft Windows	✗	✗	✓

Vulnerability Details

#1 Microsoft's September 2024 Patch Tuesday includes security updates for a total of 79 vulnerabilities, comprising 7 critical, 71 important, and 1 moderate-severity vulnerability. The breakdown of these vulnerabilities includes 30 Elevation of Privilege, 23 Remote Code Execution, 11 Information Disclosure, 8 Denial of Service, 4 Security Feature Bypass, and 3 Spoofing vulnerabilities.

#2 The updates cover a wide range of Microsoft products such as Windows, Office, Windows Hyper-V, Windows DHCP Server, Microsoft Streaming Service, Azure, Microsoft Office SharePoint, and other components. No browser vulnerabilities were addressed in this Patch Tuesday. This advisory pertains to 23 CVEs that could potentially be exploited.

#3 The updates address five zero-day vulnerabilities that are actively being exploited in the wild. The first zero-day vulnerability, CVE-2024-38014, is a Windows Installer Elevation of Privilege vulnerability that allows an attacker to gain SYSTEM privileges if successfully exploited.

#4 The second zero-day vulnerability, CVE-2024-38217, is a Windows Mark of the Web Security Feature Bypass vulnerability, which attackers have exploited since 2018. An attacker can host a malicious file to exploit this vulnerability, requiring the user to download and open the file, potentially bypassing the Mark of the Web security feature.

#5 CVE-2024-38226, a Microsoft Publisher Security Features Bypass vulnerability, is the third zero-day vulnerability patched. This vulnerability allows an attacker to bypass Office macro policies that block untrusted files, enabling exploitation through social engineering.

#6 The fourth zero-day vulnerability, CVE-2024-43491, is a critical Microsoft Windows Update Remote Code Execution vulnerability that allows remote code execution by exploiting a flaw in the Servicing Stack, affecting Windows 10 version 1507.

#7 The fifth zero-day, CVE-2024-43461, is a critical spoofing vulnerability in the Windows MSHTML platform. It was actively exploited by the Void Banshee APT group to hide malicious file extensions and deliver information-stealing malware like Atlantida. Attackers used encoded braille whitespace characters to disguise files, making them appear harmless.

#8 Four critical vulnerabilities were identified in Microsoft SharePoint, all of which could enable remote code execution. These vulnerabilities CVE-2024-38018, CVE-2024-38227, CVE-2024-38228, and CVE-2024-43464 could potentially allow attackers to execute arbitrary code on SharePoint servers. Although authentication is required for exploitation, these flaws still pose significant security risks.

#9

Other notable vulnerabilities include multiple elevation of privilege flaws in the Windows Kernel and Graphics Components, which could grant attackers SYSTEM privileges upon exploitation. The September Patch Tuesday highlights the need for timely patching to mitigate these risks, especially those being actively exploited, ensuring system integrity and protection.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38014	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-269
CVE-2024-38217	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-693
CVE-2024-38226	Microsoft Publisher 2016 Microsoft Office LTSC 2021 Microsoft Office 2019	cpe:2.3:a:microsoft:publisher:*:*:*:*:*:*:*:*	CWE-693
CVE-2024-43491	Windows 10	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-38018	Microsoft SharePoint Server: 2019 Microsoft SharePoint Server Subscription Edition: All versions Microsoft SharePoint Enterprise Server: 2016	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:*:*:*	CWE-502
CVE-2024-38227	Microsoft SharePoint Server: 2019 Microsoft SharePoint Server Subscription Edition: All versions Microsoft SharePoint Enterprise Server: 2016	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:*:*:*	CWE-77
CVE-2024-38228	Microsoft SharePoint Server: 2019 Microsoft SharePoint Server Subscription Edition: All versions Microsoft SharePoint Enterprise Server: 2016	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:*:*:*	CWE-77

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38237	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2024-38238	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2024-38241	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-38242	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-122
CVE-2024-38243	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-38244	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-38245	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-38246	Windows: 10 - 11 23H2 Windows Server: 2022 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-121

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38247	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-415
CVE-2024-38249	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-38252	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-38253	Windows: 11 – 11 24H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-416
CVE-2024-43457	Windows 11 Version 24H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-428
CVE-2024-43461	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-451
CVE-2024-43464	Microsoft SharePoint Server: 2019 Microsoft SharePoint Server Subscription Edition: All versions Microsoft SharePoint Enterprise Server: 2016	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:*:*:*:*	CWE-502
CVE-2024-43487	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-693

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 actively exploited zero-day vulnerabilities, especially CVE-2024-38014, CVE-2024-38217, CVE-2024-38226, and CVE-2024-43491, which have also been added to the CISA KEV catalog. These vulnerabilities have the potential for severe exploitation 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

TA0004 Privilege Escalation	**TA0042** Resource Development	**TA0003** Persistence	**TA0002** Execution
TA0005 Defense Evasion	**TA0004** Privilege Escalation	**T1588** Obtain Capabilities	**T1588.005** Exploits
T1059 Command and Scripting Interpreter	**T1588.006** Vulnerabilities	**T1068** Exploitation for Privilege Escalation	**T1203** Exploitation for Client Execution
T1553 Subvert Trust Controls	**T1133** External Remote Services	**T1137** Office Application Startup	**T1553.005** Mark-of-the-Web Bypass
T1204.002 Malicious File	**T1204** User Execution		

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38226

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38018

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38227

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38228

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38237

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38238

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38241

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38242

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38243

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38244

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38245

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38246

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38247

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38249

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38252

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38253

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43457

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43461

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43464

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43487

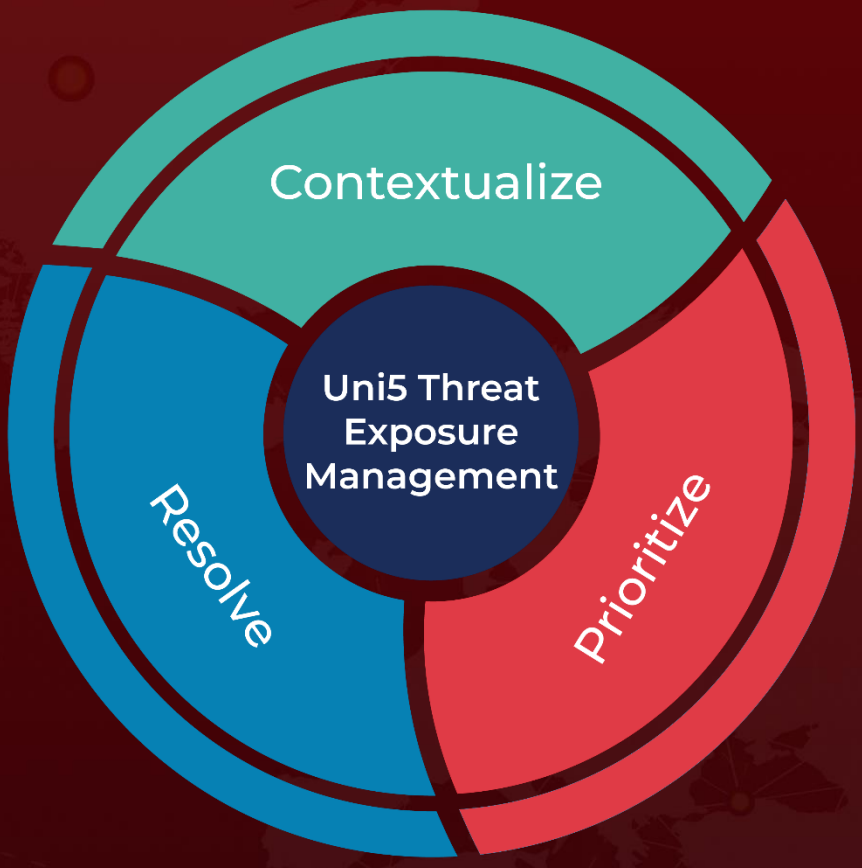
References

https://msrc.microsoft.com/update-guide/releaseNote/2024-Sep

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

September 12, 2024 . 3:30 AM

More at www.hivepro.com