Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's March 2024 Patch Tuesday Addresses 60 Vulnerabilities

Date of Publication	Last updated date	Admiralty Code	TA Number
March 13, 2024	June 13, 2024	A1	TA2024097

Summary

First Seen: March 12, 2024
Affected Platforms: Windows Hyper-V, Windows Print Spooler, Windows Graphics Component, Windows Cloud Files Mini Filter Driver, Windows Composite Image File System (CimFS), Windows Kernel, Windows Compressed Folder, Microsoft Exchange Server, Microsoft SharePoint Server
Impact: Denial of Service (DoS), Elevation of Privilege (EoP), Tampering, and Information Disclosure, Remote Code Execution (RCE)

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-21407	Windows Hyper-V Remote Code Execution Vulnerability	Windows Hyper-V	✗	✗	✓
CVE-2024-21408	Windows Hyper-V Denial of Service Vulnerability	Windows Hyper-V	✗	✗	✓
CVE-2024-21433	Windows Print Spooler Elevation of Privilege Vulnerability	Windows Print Spooler	✗	✗	✓
CVE-2024-21437	Windows Graphics Component Elevation of Privilege Vulnerability	Windows Graphics Component	✗	✗	✓
CVE-2024-26160	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability	Windows Cloud Files Mini Filter Driver	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-26170	Windows Composite Image File System (CimFS) Elevation of Privilege Vulnerability	Windows Composite Image File System (CimFS)	✗	✗	✓
CVE-2024-26182	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	✗	✗	✓
CVE-2024-26185	Windows Compressed Folder Tampering Vulnerability	Windows Compressed Folder	✗	✗	✓
CVE-2024-26198	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2024-26169	Windows Error Reporting Service Elevation of Privilege Vulnerability	Microsoft Windows	✓	✗	✓
CVE-2024-21426	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server	✗	✗	✓

Vulnerability Details

#1

Microsoft's March 2024 Patch Tuesday includes security updates for a total of 60 vulnerabilities, comprising two critical, 57 important, and one moderate vulnerability. The breakdown of vulnerabilities includes 24 Elevation of Privilege, 18 Remote Code Execution, 5 Information Disclosure, 3 Security Feature Bypass, 6 Denial of Service, 1 Tampering, and 3 Spoofing vulnerabilities.

#2

The updates cover various Microsoft products such as Office, SQL Server, .NET, Azure, Defender for Endpoint, Windows Kernel, Windows Hyper-V, Windows Print Spooler, Windows Graphics Component, Windows Cloud Files Mini Filter Driver, Windows Composite Image File System (CimFS), Windows Compressed Folder, Microsoft Exchange Server, Microsoft SharePoint Server, and more. Notably, Microsoft patched four vulnerabilities in the Chromium-based Microsoft Edge browser, bringing the total number of CVEs to 64. This advisory pertains to 10 CVEs that could potentially be exploited.

#3

One of the critical patches, CVE-2024-21407, is a remote code execution vulnerability in Windows Hyper-V, with a CVSS score of 8.1. This vulnerability allows an authenticated attacker within a guest VM to send carefully crafted file operation requests to hardware resources, potentially leading to remote code execution on the host server. Exploiting it requires prior knowledge of the environment and additional preparatory steps.

#4

CVE-2024-21408 is another critical denial of service vulnerability in Windows Hyper-V, which is a native hypervisor in Windows capable of creating virtual machines on x86-64 systems running Windows. CVE-2024-21433 is an elevation of privilege vulnerability in Windows Print Spooler. This vulnerability requires an attacker to win a race condition, upon successful exploitation the attacker can gain SYSTEM privileges.

#5

Additional notable vulnerabilities include CVE-2024-21437, CVE-2024-26170, and CVE-2024-26182, which are elevation of privilege vulnerabilities in Windows Graphics Component, Composite Image File System, and Kernel respectively, granting SYSTEM privilege. CVE-2024-26169, a vulnerability in the Windows Error Reporting Service, is believed to have been exploited by the Black Basta ransomware group as a zero-day before a patch was available.

#6

CVE-2024-26160 exposes Kernel memory via Windows Cloud Files Mini Filter Driver, while CVE-2024-26185 requires user interaction to exploit a tampering vulnerability in Windows Compressed Folder. These vulnerabilities highlight the diverse range of threats addressed in this update.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21407	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-21408	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 ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21433	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-362
CVE-2024-21437	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-264
CVE-2024-26160	Windows Server: 2019 - 2022 23H2 Windows: 10 - 11 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-200
CVE-2024-26170	Windows Server: 2019 - 2022 23H2 Windows: 10 - 11 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-264
CVE-2024-26182	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-264
CVE-2024-26185	Windows: 10 - 11 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-20
CVE-2024-26198	Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 - 2019 RTM Mar21SU 15.02.0221.018	cpe:2.3:a:microsoft:exchange_server:2016:*:*:*:*:*:*:*	CWE-427
CVE-2024-26169	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-269

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21426	Microsoft SharePoint Server: 2019 Microsoft SharePoint Server Subscription Edition: All versions Microsoft SharePoint Enterprise Server: 2016	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_server:subscription_edition:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_enterprise_server:*:*:*:*:*:*:*:*	CWE-20

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 critical vulnerabilities, especially CVE-2024-21407 (Windows Hyper-V Remote Code Execution Vulnerability) and CVE-2024-21408 (Windows Hyper-V Denial of Service Vulnerability). 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	TA0007 Discovery	TA0002 Execution
TA0003 Persistence	TA0005 Defense Evasion	TA0040 Impact	T1588.005 Exploits
T1059 Command and Scripting Interpreter	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation	T1203 Exploitation for Client Execution
T1082 System Information Discovery	T1566 Phishing	T1588 Obtain Capabilities	T1498 Network Denial of Service

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	4aae231fb5357c0647483181aeae47956ac66e42b6b134f5b90da76d8ec0ac63, b73a7e25d224778172e394426c98b86215087d815296c71a3f76f738c720c1b0, a31e075bd5a2652917f91714fea4d272816c028d7734b36c84899cd583181b3d, 3b3bd81232f517ba6d65c7838c205b301b0f27572fcfef9e5b86dd30a1d55a0d, 2408be22f6184cdccec7a34e2e79711ff4957e42f1ed7b7ad63f914d37dba625, b0903921e666ca3ffd45100a38c11d7e5c53ab38646715eafc6d1851ad41b92e, 71d50b74f81d27feefbc2bc0f631b0ed7fcdf88b1abbd6d104e66638993786f8, 0f9156f91c387e7781603ed716dcdc3f5342ece96e155115708b1662b0f9b4d0, 1ad05a4a849d7ed09e2efb38f5424523651baf3326b5f95e05f6726f564ccc30, 93058bd5fe5f046e298e1d3655274ae4c08f07a8b6876e61629ae4a0b510a2f7, 1cb1864314262e71de1565e198193877ef83e98823a7da81eb3d59894b5a4cfb

TYPE	VALUE
Domains	upd7a[.]com, upd7[.]com, upd9[.]com, upd5[.]pro, antispam3[.]com, antispam2[.]com, instance-olqdnn-relay.screenconnect[.]com, greekpool[.]com, zziveastnews[.]com, realsepnews[.]com

Patch Details

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21407

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21408

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21433

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21437

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26160

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26170

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26182

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26185

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26198

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21426

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26169

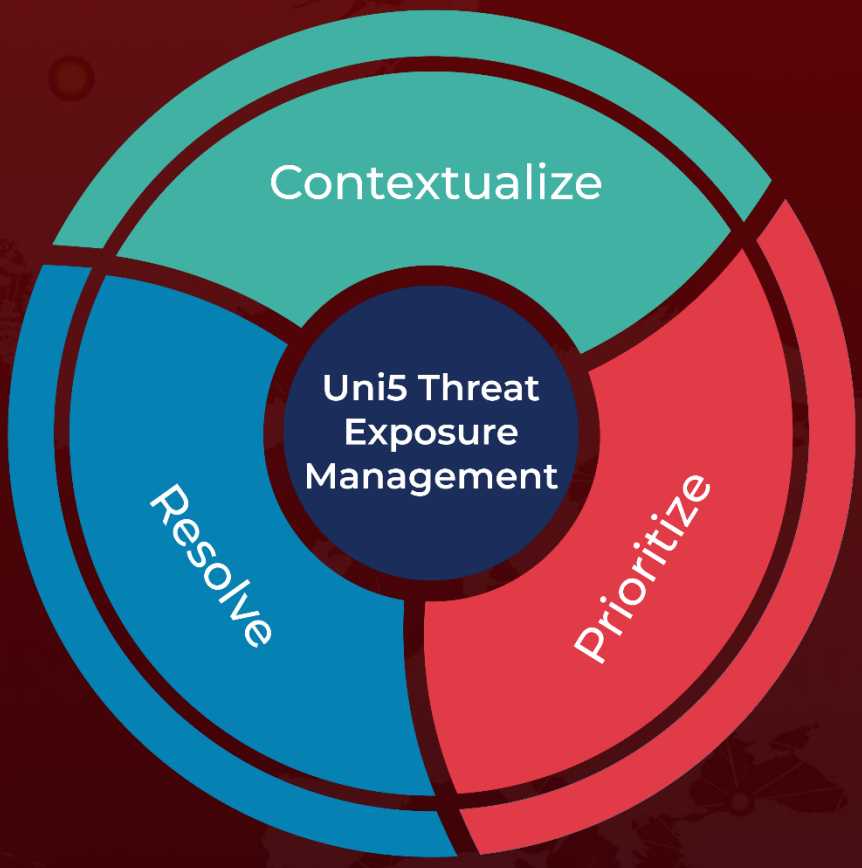
References

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

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

March 13, 2024 • 8:30 AM

More at www.hivepro.com