Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's May 2023 update addresses two Zero-Day Vulnerabilities

Date of Publication	Admiralty Code	TA Number
May 10, 2023	A1	TA2023220

Summary

First Seen: May 10, 2023
Affected Product: Microsoft SharePoint Server, Windows & Windows Server
Impact: Remote Code Execution and Privilege Escalation

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-24902	Win32k Elevation of Privilege Vulnerability	Windows	✗	✗	✓
CVE-2023-24941	Windows Network File System Remote Code Execution Vulnerability	Windows Server	✗	✗	✓
CVE-2023-24949	Windows Kernel Elevation of Privilege Vulnerability	Windows & Windows Server	✗	✗	✓
CVE-2023-24950	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft SharePoint Server	✗	✗	✓
CVE-2023-24954	Microsoft SharePoint Server Information Disclosure Vulnerability	Microsoft SharePoint Server	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-24955	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server	✗	✗	✓
CVE-2023-29324	Windows MSHTML Platform Security Feature Bypass Vulnerability	Windows & Windows Server	✗	✗	✓
CVE-2023-29325	Windows OLE Remote Code Execution Vulnerability	Windows & Windows Server	✗	✗	✓
CVE-2023-29336	Win32k Elevation of Privilege Vulnerability	Windows & Windows Server	✓	✓	✓
CVE-2023-24932	Secure Boot Security Feature Bypass Vulnerability	Windows & Windows Server	✓	✗	✓

Vulnerability Details

#1 Microsoft released a security update in May 2023 to address 40 CVEs, including two zero-day vulnerabilities that have already been exploited in the wild. The two zero-day vulnerabilities are the Win32k Elevation of Privilege Vulnerability(CVE-2023-29336) and Secure Boot Security Feature Bypass Vulnerability(CVE-2023-24932)

#2 In addition to these, other vulnerabilities addressed in the update include Windows Kernel Elevation of Privilege Vulnerability, Microsoft SharePoint Server Spoofing Vulnerability, Microsoft SharePoint Server Information Disclosure Vulnerability, Microsoft SharePoint Server Remote Code Execution Vulnerability, Windows MSHTML Platform Security Feature Bypass Vulnerability, and Windows OLE Remote Code Execution Vulnerability.

#3 The Win32k Elevation of Privilege Vulnerability could allow an attacker to gain elevated privileges on a compromised system, potentially enabling them to execute arbitrary code, install malicious software, or perform other malicious activities. The Windows Network File System Remote Code Execution Vulnerability could allow an attacker to execute arbitrary code on a vulnerable system and take control of it.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-24902	Windows: 11 - 11 22H2, 10 - 10 S	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-264
CVE-2023-24941	Windows Server: 2012 - 2022 20H2	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-20
CVE-2023-24949	Windows: 10 - 10 S, 11 - 11 22H2; Windows Server: 2019 - 2022 20H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-264
CVE-2023-24950	Microsoft SharePoint Server: 2019; Microsoft SharePoint Server Subscription Edition: All versions; Microsoft SharePoint Enterprise Server: 2016	cpe:2.3:a:microsoft:microsoft_sharepoint_server:*:*:*:*:*:*:*:*	CWE-451
CVE-2023-24954			CWE-200
CVE-2023-24955			CWE-20
CVE-2023-29324	Windows: 10 - 10 S, 11 - 11 22H2; Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-254
CVE-2023-29325			CWE-362

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-29336	Windows: 10 - 10 S; Windows Server: 2008 - 2016	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-119
CVE-2023-24932	Windows: 10 - 10 S, 11 - 11 22H2; Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-254

Recommendations

Apply the May 2023 security update from Microsoft as soon as possible to address the 40 CVEs, including the two zero-day vulnerabilities. Ensure that your system is set up to receive automatic updates, so you don't miss any future security patches.

Use up-to-date antivirus software to detect and block any potential threats. Regularly back up your important files to a secure location, so you can recover them if your system is compromised. Use strong and unique passwords for all your accounts and enable two-factor authentication whenever possible.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement	TA0011 Command and Control
TA0040 Impact	T1574 Hijack Execution Flow	T1059 Command and Scripting Interpreter	T1027 Obfuscated Files or Information
T1499 Endpoint Denial of Service	T1033 System Owner/User Discovery	T1550 Use Alternate Authentication Material	T1135 Network Share Discovery

T1090 Proxy	T1195 Supply Chain Compromise	T1217 Browser Bookmark Discovery	T1018 Remote System Discovery
T1124 System Time Discovery	T1046 Network Service Discovery	T1016 System Network Configuration Discovery	T1082 System Information Discovery
T1083 File and Directory Discovery	T1057 Process Discovery	T1007 System Service Discovery	T1087 Account Discovery
T1069 Permission Groups Discovery			

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24902

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24941

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24949

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24950

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24954

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24955

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29324

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29325

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29336

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24932

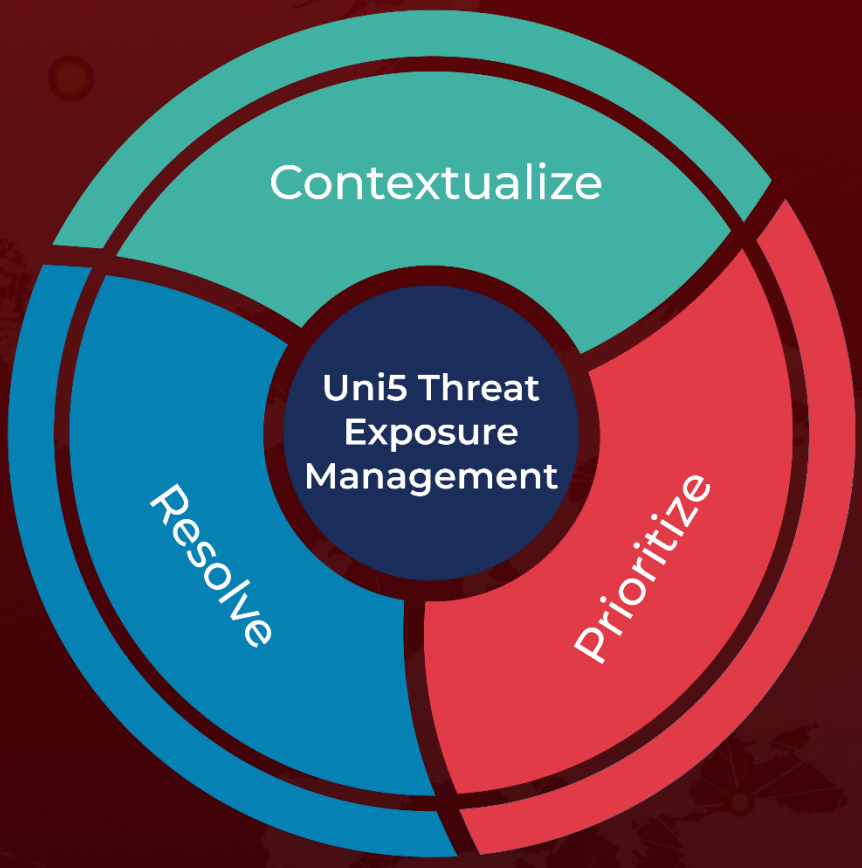
References

https://msrc.microsoft.com/update-guide/releaseNote/2023-May

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

May 10, 2023 • 6:50 AM

More at www.hivepro.com