Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft tackles three actively exploited zero-day vulnerabilities and several other bugs

Date of Publication	Admiralty Code	TA Number
February 15, 2023	A1	TA2023082

Summary

First Seen: February 14, 2023
Affected Product: Microsoft Windows, Exchange Server, and Sharepoint
Impact: Remote Code Execution, Privilege Escalation, Information Disclosure, Spoofing, Security Feature Bypass, and Denial of Service.

CVEs

CVE	NAME	PATCH
CVE-2023-21823*	Windows Graphics Component Remote Code Execution Vulnerability	✓
CVE-2023-21715*	Microsoft Publisher Security Features Bypass Vulnerability	✓
CVE-2023-23376*	Windows Common Log File System Driver Elevation of Privilege Vulnerability	✓
CVE-2023-21808	.NET and Visual Studio Remote Code Execution Vulnerability	✓
CVE-2023-21716	Microsoft Word Remote Code Execution Vulnerability	✓
CVE-2023-21718	Microsoft SQL ODBC Driver Remote Code Execution Vulnerability	✓
CVE-2023-21815	Visual Studio Remote Code Execution Vulnerability	✓

*zero-day vulnerability

CVE	NAME	PATCH
CVE-2023-21803	Windows iSCSI Discovery Service Remote Code Execution Vulnerability	✓
CVE-2023-21717	Microsoft SharePoint Server Elevation of Privilege Vulnerability	✓
CVE-2023-21777	Azure App Service on Azure Stack Hub Elevation of Privilege Vulnerability	✓
CVE-2023-21806	Power BI Report Server Spoofing Vulnerability	✓
CVE-2023-21804	Windows Graphics Component Elevation of Privilege Vulnerability	✓
CVE-2023-21819	Windows Secure Channel Denial of Service Vulnerability	✓
CVE-2023-21689	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability	✓
CVE-2023-21688	NT OS Kernel Elevation of Privilege Vulnerability	✓
CVE-2023-23381	Visual Studio Remote Code Execution Vulnerability	✓
CVE-2023-21690	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability	✓

Vulnerability Details

#1

The February Patch Tuesday addresses three zero-day vulnerabilities. One of these vulnerabilities is an Elevation of Privilege Vulnerability in the Microsoft Windows Graphics Component, which has been actively exploited in the wild and is tracked as CVE-2023-21823. To exploit this weakness, an attacker must log into a vulnerable machine and run a specially created program. If successfully exploited, an attacker would be able to run processes in an elevated context.

#2

A Security Features Bypass vulnerability in Microsoft Publisher is the second zero-day vulnerability. Exploiting CVE-2023-21715 allows an attacker to bypass Office macro security measures using a specially designed document and execute code that would otherwise be blocked by policy. This can deceive the user into opening the file and executing arbitrary code on the system.

#3

The Windows Common Log File System Driver Elevation of Privilege Vulnerability, designated as CVE-2023-23376, is the third vulnerability currently being actively exploited. This vulnerability is caused by a boundary error in the Windows Common Log File System Driver, which can be triggered by a local user. If exploited, this vulnerability can result in memory corruption and enable arbitrary code to be executed with SYSTEM privileges.

#4

The flaw in Power BI, designated as CVE-2023-21806, allows a remote attacker to launch a spoofing attack. This vulnerability exists due to incorrectly processed user-supplied data, which can deceive the victim into opening a malicious file and then spoof it. The Windows ALPC vulnerability, designated as CVE-2023-21688, allows a local user to gain elevated system access. The vulnerability is caused by a boundary mistake within the NT OS Kernel. If a local user with SYSTEM access exploits this vulnerability, they can cause memory corruption and execute arbitrary code.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-21823	Windows: 10 - 11 22H2 & Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*	CWE-119
CVE-2023-21715	Microsoft Office: 365 & Microsoft Publisher: 1912 12325.20264 - 2301 16026.20170	cpe:2.3:a:microsoft:microsoft_office:365:*:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_publisher:-:*:*:*:*:*:*:*	CWE-254
CVE-2023-23376	Windows: 10 - 11 22H2 & Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*	CWE-119
CVE-2023-21808	Visual Studio: 15.9 - 17.4.4 17.4.33213.308, Microsoft .NET Framework: 3.5 - 4.8.1 & Microsoft .NET Core: 6.0.0 - 7.0.2	cpe:2.3:a:microsoft:visual_studio:-:*:*:*:*:*:*:*	CWE-20
CVE-2023-21716	Microsoft Office: 365 – 2021 & Microsoft Word: before 16.0.16026.20200	cpe:2.3:a:microsoft:microsoft_office:-:*:*:*:*:*:*:*	CWE-119
CVE-2023-21718	Microsoft SQL Server: 2014 12.0.2000.8 - 2022 RC1 16.0.950.9	cpe:2.3:a:microsoft:microsoft_sql_server:-:*:*:*:*:*:*	CWE-20
CVE-2023-21815	Visual Studio: 15.0 26228.04 - 17.4.4 17.4.33213.308	cpe:2.3:a:microsoft:visual_studio:-:*:*:*:*:*:*:*	CWE-119
CVE-2023-21803	Windows: 10 - 10 1809 & Windows Server: 2008 - 2008 SP2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*	CWE-20
CVE-2023-21717	Microsoft SharePoint Server: 2013 - 2019 & Microsoft SharePoint Server: 2013	cpe:2.3:a:microsoft:microsoft_sharepoint_server:-:*:*:*:*:*:*:*	CWE-284
CVE-2023-21777	Azure App Service on Azure Stack Hub: All versions	cpe:2.3:a:microsoft:azure_app_service_on_azure_stack_hub:*:*:*:*:*:*:*:*	CWE-94

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-21806	Power BI Report Server: 14.0.600.271 - 15.0.1110.135	cpe:2.3:a:microsoft:power_bi_report_server:-:*:*:*:*:*:*:*	CWE-451
CVE-2023-21804	Windows: 10 - 11 22H2 & Windows Server: 2012 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*	CWE-119
CVE-2023-21819	Windows: 10 20H2 - 11 22H2 & Windows Server: 2019 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*	CWE-20
CVE-2023-21689	Windows: 10 - 11 22H2 & Windows Server: 2008 R2 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*	CWE-20
CVE-2023-21688	Windows: 10 - 11 22H2 & Windows Server: 2008 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*	CWE-119
CVE-2023-23381	Visual Studio: 15.9 - 17.4.4 17.4.33213.308	cpe:2.3:a:microsoft:visual_studio:-:*:*:*:*:*:*:	CWE-119
CVE-2023-21690	Windows: 10 - 11 22H2 & Windows Server: 2008 R2 - 2022 20H2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*	CWE-20

Recommendations

Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0040 Impact	TA0043 Reconnaissance	T1556 Modify Authentication Process
T1203 Exploitation for Client Execution	T1036 Masquerading	T1082 System Information Discovery	T1068 Exploitation for Privilege Escalation
T1210 Exploitation of Remote Services	T1592 Gather Victim Host Information	T1190 Exploit Public-Facing Application	T1499 Endpoint Denial of Service

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21823
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21715
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23376
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21808
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21716
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21718
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21815
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21803
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21717
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21777
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21806
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21804
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21819
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21689
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21688
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23381
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21690

References

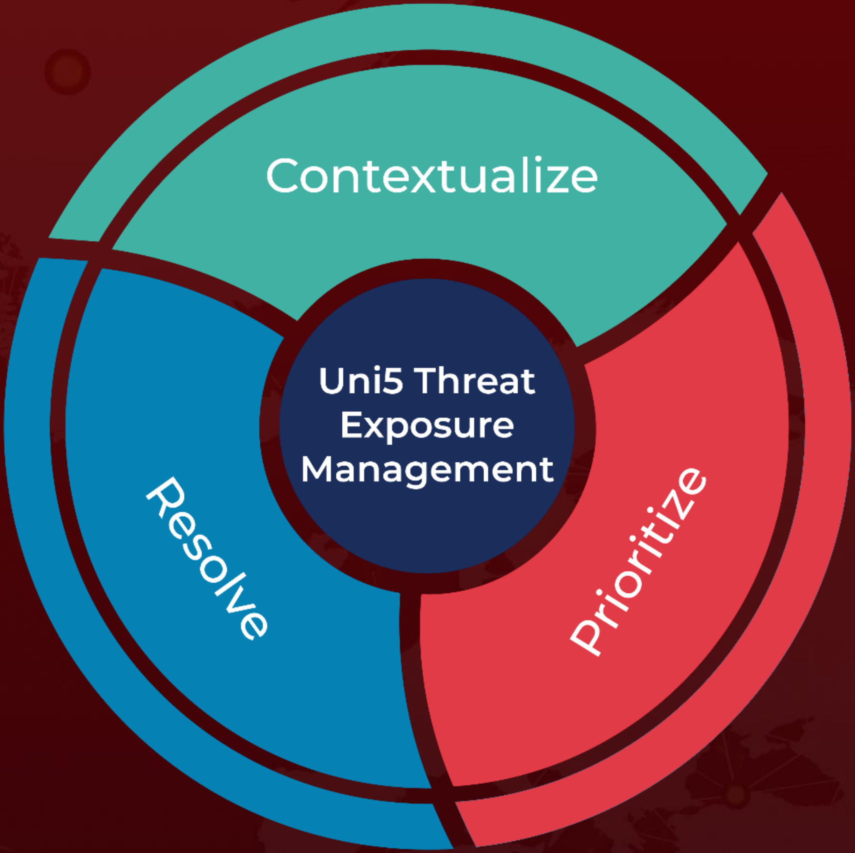
https://msrc.microsoft.com/update-guide/releaseNote/2023-Feb

https://blog.qualys.com/vulnerabilities-threat-research/patch-tuesday/2023/02/14/the-february-2023-patch-tuesday-security-update-review

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 15, 2023 • 3:49 AM

More at www.hivepro.com