Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft fixed 83 vulnerabilities including two zero-day vulnerabilities

Date of Publication	Admiralty Code	TA Number
March 15, 2023	A1	TA2023136

Summary

First Seen: March 14, 2023
Affected Product: Microsoft Office and Components, Microsoft Dynamics, Microsoft OneDrive, Microsoft Windows Codecs Library, Client Server Runtime Subsystem (CSRSS), Internet Control Message Protocol (ICMP), Microsoft PostScript Printer Driver.
Impact: Remote Code Execution, Privilege Escalation, Information Disclosure, Spoofing, Security Feature Bypass, and Denial of Service.

CVEs

CVE	NAME	PATCH	CISA
CVE-2023-23415	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability	✓	✗
CVE-2023-23397*	Microsoft Outlook Elevation of Privilege Vulnerability	✓	✓
CVE-2023-23404	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability	✓	✗
CVE-2023-23411	Windows Hyper-V Denial of Service Vulnerability	✓	✗
CVE-2023-23416	Windows Cryptographic Services Remote Code Execution Vulnerability	✓	✗
CVE-2023-23392	HTTP Protocol Stack Remote Code Execution Vulnerability	✓	✗
CVE-2023-21708	Remote Procedure Call Runtime Remote Code Execution Vulnerability	✓	✗
CVE-2023-1017	TPM2.0 Module Library Elevation of Privilege Vulnerability	✓	✗
CVE-2023-1018	TPM2.0 Module Library Elevation of Privilege Vulnerability	✓	✗
CVE-2023-24880*	Windows SmartScreen Security Feature Bypass Vulnerability	✓	✓

* Represents zero-day vulnerability

Vulnerability Details

#1 Microsoft has released its March 2023 Patch Tuesday update, addressing a total of 83 vulnerabilities, including 9 critical, 70 important, 1 moderate, and 3 other vulnerabilities. The update also includes fixes for two zero-day vulnerabilities that were actively exploited in the wild. Microsoft has also fixed several other vulnerabilities, including DoS, EoP, Information Disclosure, RCE, Security Feature Bypass, and Spoofing in its software. This report highlights 10 critical vulnerabilities that were included in the update.

#2 The first zero-day vulnerability (CVE-2023-23397) was exploited by STRONTIUM, a state-sponsored Russian hacking group, to steal emails for specific accounts. The vulnerability allowed external attackers to send specially crafted emails that would cause a connection from the victim's device to an external UNC location under the attacker's control, which leaked the victim's Net-NTLMv2 hash to the attacker.

#3 The second zero-day vulnerability (CVE-2023-24880) was exploited by the Magniber ransomware operation to bypass the Windows Mark of the Web security warning. This vulnerability allowed attackers to craft a malicious file that evades Mark of the Web defenses, resulting in a limited loss of integrity and availability of security features such as Protected View in Microsoft Office that rely on MOTW tagging. Microsoft has fixed the vulnerabilities in the update and urged users to install the latest security patches to stay protected from these vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-23415	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	CWE-20
CVE-2023-23397*	Microsoft Outlook: 2013 - 2021 Microsoft Office: 365 - 2021	cpe:2.3:a:microsoft:microsoft_outlook:2016:*:*:*:*:*:*:*	CWE-200
CVE-2023-23404	Windows: 10 - 11 22H2 Windows Server: 2012 - 2022	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	CWE-362
CVE-2023-23411	Windows: 10 - 11 22H2 Windows Server: 2016 - 2022	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	CWE-20

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-23416	Windows: 10 - 11 22H2 Windows Server: 2012 - 2022	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	CWE-20
CVE-2023-23392	Windows Server: 2022 - 2022 20H2 Windows: 11 - 11 22H2 Microsoft IIS: 10.0	cpe:2.3:o:microsoft:windows_server:2022:*:*:*:*:*:*:*	CWE-20
CVE-2023-21708	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	CWE-20
CVE-2023-1017	Windows: 10 - 11 22H2 Windows Server: 2016 - 2019 2004	cpe:2.3:o:microsoft:windows:10:22H2:*:*:*:*:*:*:*	CWE-787
CVE-2023-1018	Windows: 10 - 11 22H2 Windows Server: 2016 - 2022	cpe:2.3:o:microsoft:windows:10:22H2:*:*:*:*:*:*:*	CWE-125
CVE-2023-24880*	Windows: 10 - 11 22H2 Windows Server: 2016 - 2022 20H2	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	CWE-254

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

TA0005 Defense Evasion	TA0004 Privilege Escalation	TA0002 Execution	TA0040 Impact
TA0003 Persistence	T1499 Endpoint Denial of Service	T1036 Masquerading	T1190 Exploit Public-Facing Application
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	T1140 Deobfuscate/Decode Files or Information
T1203 Exploitation for Client Execution	T1546 Event Triggered Execution	T1546.008 Accessibility Features	T1068 Exploitation for Privilege Escalation

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23415

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23397

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23404

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23411

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23416

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23392

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21708

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-1017

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-1018

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24880

References

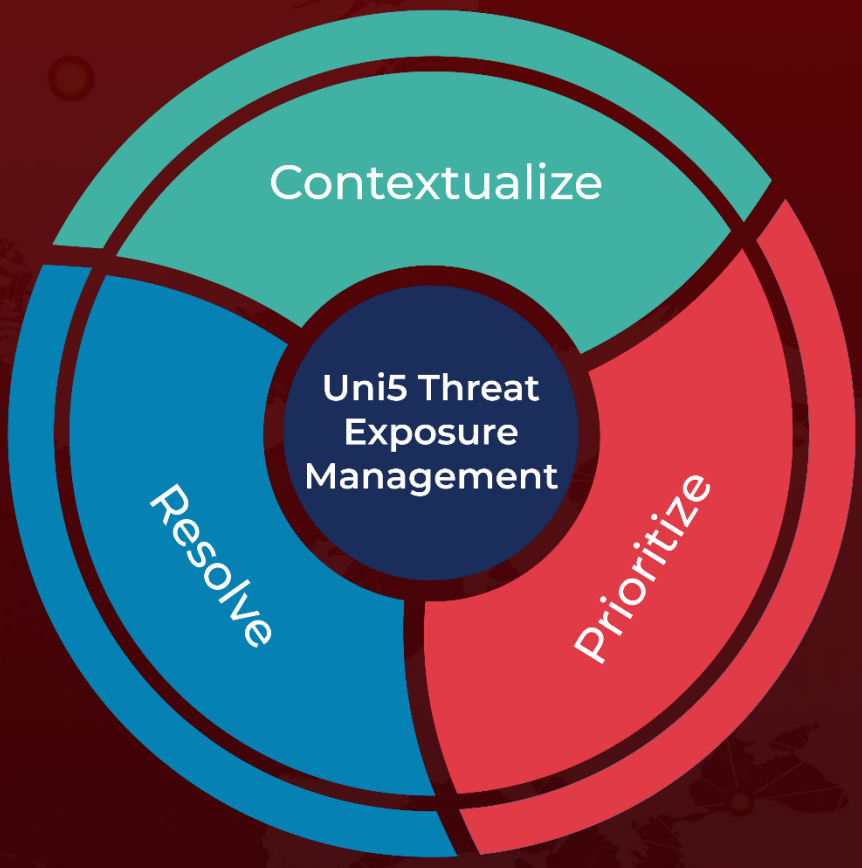
https://msrc.microsoft.com/update-guide/releaseNote/2023-Mar

https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2023-patch-tuesday-fixes-2-zero-days-83-flaws/

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 15, 2023 • 04:30 AM

More at www.hivepro.com