Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Zero-Click Outlook RCE Exploitation Chain in Windows

Date of Publication	Admiralty Code	TA Number
December 22, 2023	A1	TA2023518

Summary

First Seen: December, 2023
Affected Platform: Microsoft Windows
Impact: Two vulnerabilities (CVE-2023-35384 and CVE-2023-36710) in Microsoft Windows can be chained to achieve remote code execution (RCE) on vulnerable Outlook clients. Attackers can exploit these flaws by sending a crafted email with a custom notification sound file to trigger the download of a malicious audio file from a remote server.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-35384	Microsoft Windows HTML Platforms Security Features Bypass Vulnerability	Microsoft Windows	☒	☒	✓
CVE-2023-36710	Microsoft Windows Media Foundation Core Remote Code Execution Vulnerability	Microsoft Windows	☒	☒	✓

Vulnerability Details

#1 Two vulnerabilties in Microsoft Windows, identified as CVE-2023-35384 and CVE-2023-36710. When exploited together, these vulnerabilities enable a full, zero-click remote code execution (RCE) exploit against Outlook clients. A zero-click vulnerability is a security flaw in software that can be exploited without any interaction from the user.

#2 The first vulnerability involves the MapUrlToZone function's parsing of a path. To exploit this, a crafted email must be sent to an Outlook client, initiating the download of a specific sound file from an attacker-controlled server.

#3 The second vulnerability is found in the Audio Compression Manager (ACM) and is triggered when the downloaded sound file is autoplayed, leading to code execution on the victim's machine.

#4 Microsoft was informed of these vulnerabilities, and they were addressed in the August 2023 and October 2023 Patch Tuesdays. Windows machines with the October 2023 software update are protected, and Outlook clients using Exchange servers patched with the March 2023 update are also safeguarded.

#5 The research also delves into the background, including a previously patched Outlook vulnerability (CVE-2023-23397) exploited by a Russian state-sponsored threat actor known as Forest Blizzard. Despite fixes, the researchers discovered a bypass, leading to further investigation and the identification of the two new vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-35384	Windows: 10 - 11 22H2 Windows Server: 2012 R2 - 2022 20H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-254
CVE-2023-36710	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

Apply Microsoft Security Updates: Ensure that all Windows systems are promptly updated with the latest security patches, especially those released in August and October 2023. For Outlook clients using Exchange servers, ensure the March 2023 update is applied to protect against the abused feature.

NTLM Mitigation: Consider disabling NTLM authentication in your environment or, alternatively, add users to the Protected Users group, which restricts the use of NTLM as an authentication mechanism.

Block Outgoing SMB Connections: Implement controls to block outgoing Server Message Block (SMB) connections to remote public IP addresses. This helps prevent unauthorized access and data exfiltration.

Network Segmentation: Implement microsegmentation to restrict lateral movement within the network. This limits the potential spread of an attack in case one segment is compromised.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0042 Resource Development	T1588.006 Vulnerabilities
TA0011 Command and Control	TA0006 Credential Access	T1588 Obtain Capabilities	T1555 Credentials from Password Stores
T1566 Phishing	T1555.004 Windows Credential Manager	T1203 Exploitation for Client Execution	T1588.005 Exploits
T1659 Content Injection			

Patch Details

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36710

References

https://www.akamai.com/blog/security-research/chaining-vulnerabilities-to-achieve-rce-part-one

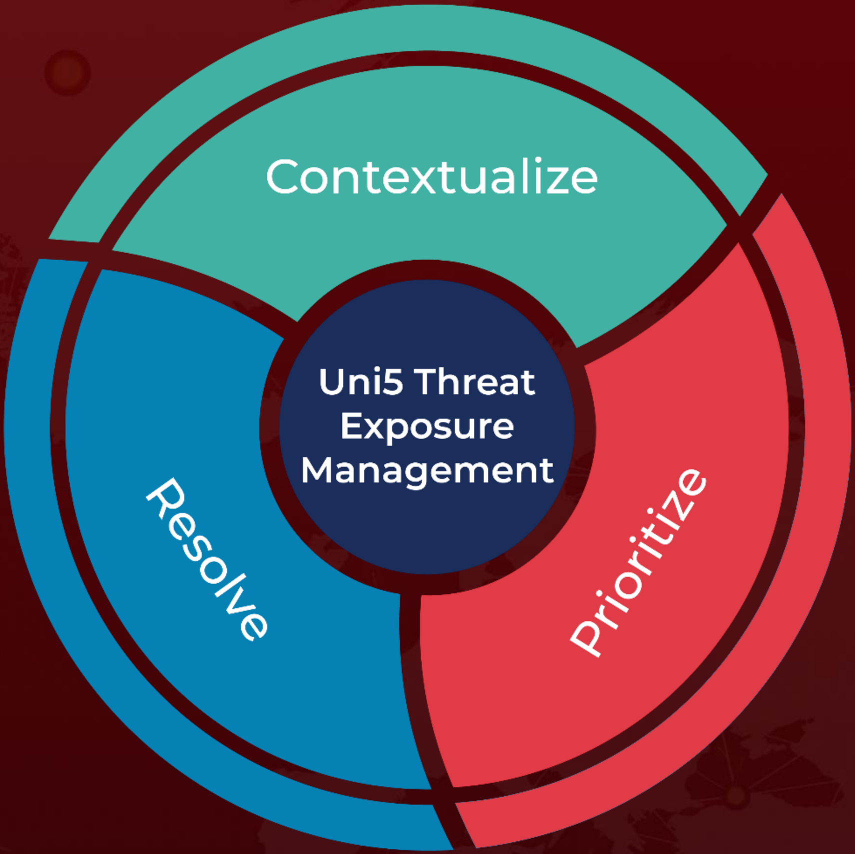
https://www.akamai.com/blog/security-research/chaining-vulnerabilities-to-achieve-rce-part-two

https://www.hivepro.com/threat-advisory/outlook-vulnerability-exploited-by-russian-hackers-since-april-2022/

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

December 22, 2023 • 4:30 AM

More at www.hivepro.com