Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

Outlook Vulnerability Exploited by Russian Hackers Since April 2022

Date of Publication	Admiralty Code	TA Number
March 17, 2023	A1	TA2023143

Summary

Attack Begin: April 2022
Attack Countries: Poland, Ukraine, Romania, and Turkey
Attack Industry: Government, Logistics, Oil/Gas, Defense, and Transportation
Attack: A vulnerability in Microsoft Outlook allowed an unknown Russian threat actor to gain access to a victim's NTLM hash through a specially crafted email.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVE

CVE	NAME	PATCH	CISA KEV
CVE-2023-23397*	Microsoft Office Outlook Privilege Escalation Vulnerability	✓	✓

* ZERO-DAY VULNERABILITY

Attack Details

#1

Starting in April 2022, an unknown Russian threat actor began exploiting a vulnerability in Microsoft Outlook, a popular email client. The vulnerability allowed the attacker to gain access to the NTLM hash of a victim, which is used for authentication in Windows environments. The attacker accomplished this by sending a specially crafted email that contained code leading to an attacker-controlled server.

#2

Once the victim received the email, Microsoft Outlook attempted to connect to the attacker's server using the victim's NTLM hash. This allowed the attacker to obtain the hash and use it to move laterally across the network. This meant that the attacker could potentially access sensitive information and perform malicious actions on the victim's machine and throughout the network. Microsoft has since released a patch for this vulnerability as part of their March 2023 Patch Tuesday update.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-23397	Microsoft Outlook: 2013 - 2021 Microsoft Office 365	cpe:2.3:a:microsoft:microsoft_outlook:2016:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:365_apps:-:*:*:*:*:*:*:*	CWE-200

Recommendations

To protect against CVE-2023-23397 attacks, it's recommended to either apply the patch or block outbound SMB (TCP port 445) and add users to the Protected Users group in Active Directory. These measures can reduce the impact of the vulnerability and minimize the risk of successful attacks.

Organizations can utilize Microsoft's documentation and script to check for any exploitation attempts of the vulnerability. This can help assess if any attacks have occurred and facilitate necessary action to mitigate the impact if needed.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0005 Defense Evasion	TA0008 Lateral Movement	TA0011 Command and Control
T1190 Exploit Public-Facing Application	T1021 Remote Services	T1021.002 SMB/Windows Admin Shares	T1550 Use Alternate Authentication Material
T1550.002 Pass the Hash	T1571 Non-Standard Port		

Patch Link

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

References

https://thestack.technology/cve-2023-23397-poc-outlook-exploit/

https://thestack.technology/critical-microsoft-outlook-vulnerability-cve-2023-23397/

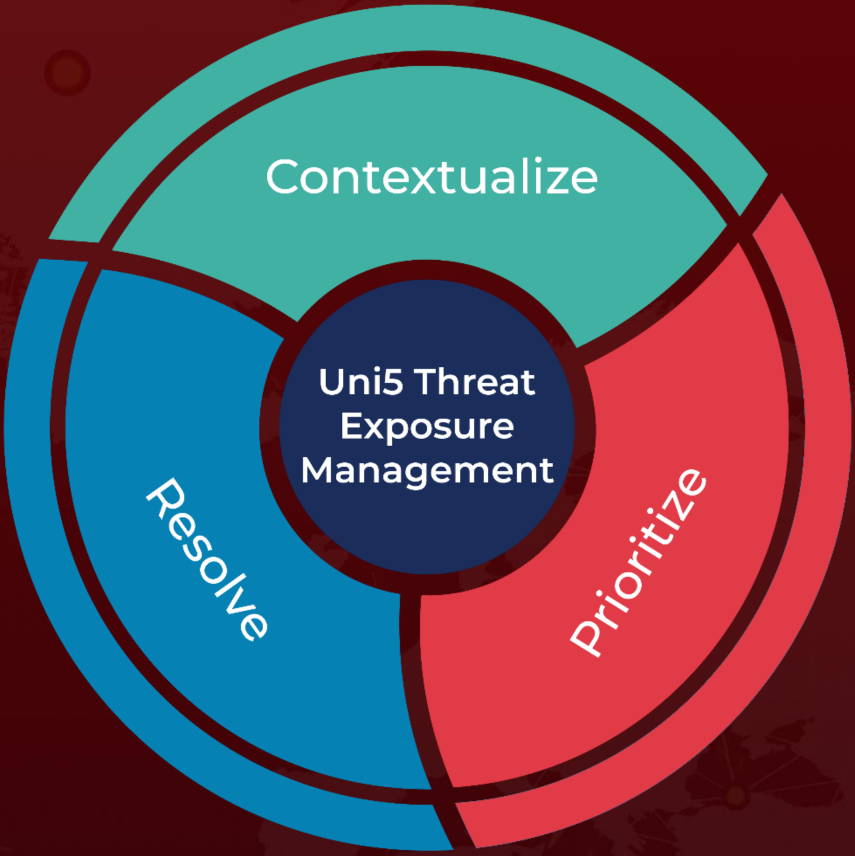
https://blog.cyble.com/2023/03/16/microsoft-outlook-zero-day-vulnerability-cve-2023-23397-actively-exploited-in-the-wild/

https://microsoft.github.io/CSS-Exchange/Security/CVE-2023-23397/

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 17, 2023 • 3:50 AM

More at www.hivepro.com