KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Russian Hackers Exploiting Microsoft Outlook's Critical Vulnerability

Tracker ID: TN2351 **Date:** April 03, 2023 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Microsoft has released guidelines to assist customers in tracking and monitoring assault attempts by a Russian Threat Actor. It has disclosed the indicators of compromise associated with a recently patched Outlook vulnerability, identified as CVE-2023-23397 with CVSS Score of 9.8. The critical flaw relates to a case of privilege escalation that could be exploited to steal NT Lan Manager (NTLM) hashes and launch a relay attack without requiring any user interaction.

Remote attackers could send tailored emails that direct the target to a malicious location under the authority of the attackers. The Microsoft Threat Intelligence team found the limited, targeted abuse of the Microsoft Outlook for Windows vulnerability that could enable new technology LAN Manager (NTLM) password transfer to an insecure network, such as the Internet.

In one attack sequence outlined by Microsoft, a successful Net-NTLMv2 Relay assault allowed the threat actor to obtain unauthorized access to an Exchange Server and alter inbox folder rights to gain continuous access. The stolen email account was then used to further the adversary's access within the breached environment by sending more malicious messages to other members of the same organization. While using NTLMv2 hashes to obtain unauthorized access to resources is not a new method, exploiting CVE-2023-23397 is innovative and covert.

Organizations should examine SMBClient event logging, Process Creation events, and other accessible network data to spot possible CVE-2023-23397 exploitation. Microsoft has issued a fix to address the critical elevation of privilege (EoP) flaw in Microsoft Outlook for Windows. To address this vulnerability, organization must install the Outlook security update, regardless of where the mail is hosted (e.g., Exchange Online, Exchange Server, some other platform) or the organization's support for NTLM authentication.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | | Russian Hackers Exploiting Microsoft Outlook's Critical Vulnerability

Tracker ID: TN2351 **Date:** April 03, 2023 **Category:** Vulnerability **Industry:** All **Region**: All

Analysis

CVE ID	Severity	CVSS Score
CVE-2023-23397	Critical	9.8

Affected Products

All supported versions of Microsoft Outlook for Windows are affected.

Note: Other versions of Microsoft Outlook such as Android, iOS, Mac, as well as Outlook on the web and other M365 services are not affected.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Administrators and organizations are encouraged refer to the Microsoft released guidance to patch.
- Ensure systems and devices are patched against the identified vulnerabilities and exploits as soon as possible.
- End users should be made aware of the latest phishing tactic employed by the threat actors and ensure not click on any suspicious URLs or emails.
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | | Russian Hackers Exploiting Microsoft Outlook's Critical Vulnerability

Tracker ID: TN2351 **Date:** April 03, 2023 **Category:** Vulnerability **Industry:** All **Region**: All

References

- Ravie Lakshmanan, Microsoft Warns of Stealthy Outlook Vulnerability Exploited by Russian Hackers, Bleeping Computer, March 24, 2023, External Link (thehackernews.com).
- Microsoft Outlook Elevation of Privilege Vulnerability, CVE-2023-23397, Security Vulnerability, Microsoft, March 21, 2023, External Link (msrc.microsoft.com).
- MSRC Blog, Microsoft Mitigates Outlook Elevation of Privilege Vulnerability, Microsoft, March 14, 2023, External Link (msrc.microsoft.com).
- Microsoft Incident Response, Guidance for investigating attacks using CVE-2023-23397, Microsoft Security, March 24, 2023, External Link (www.microsoft.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI

KPMG in India Cyber Response Hotline : +91 9176471471

IP

101.255.119[.]42
213.32.252[.]221
168.205.200[.]55
185.132.17[.]160
69.162.253[.]21
113.160.234[.]229
181.209.99[.]204
82.196.113[.]102
85.195.206[.]7
61.14.68[.]33