Russian hackers exploiting Outlook bug to hijack Exchange accounts

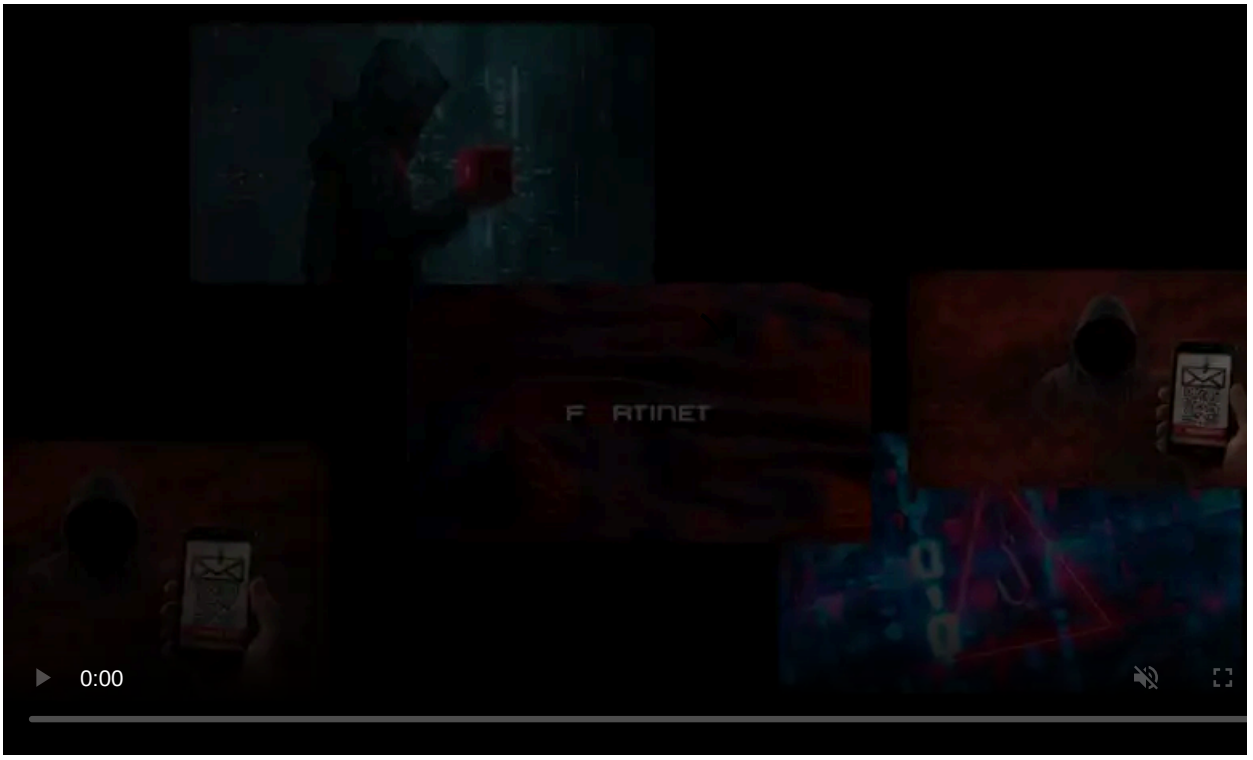
By Bill Toulas

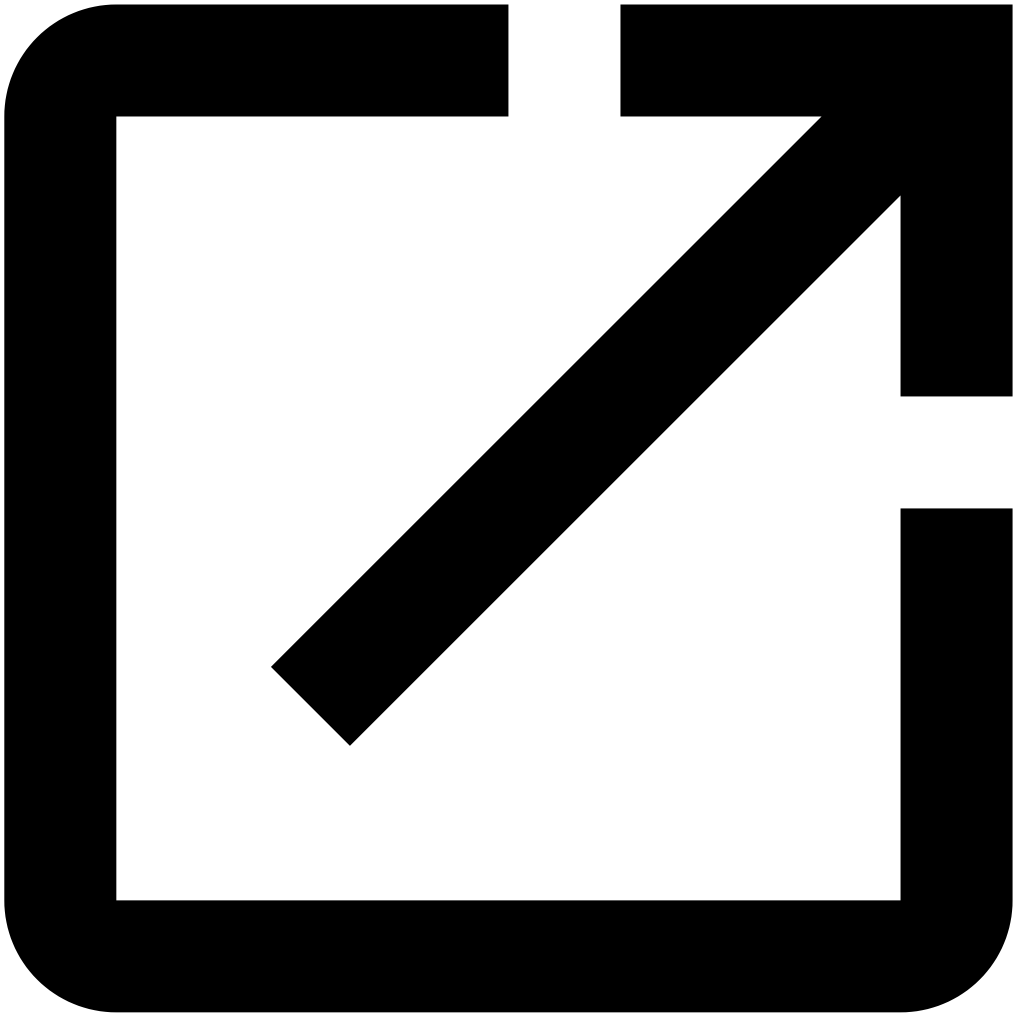
Published: 2023-12-04 · Archived: 2026-04-06 02:59:20 UTC

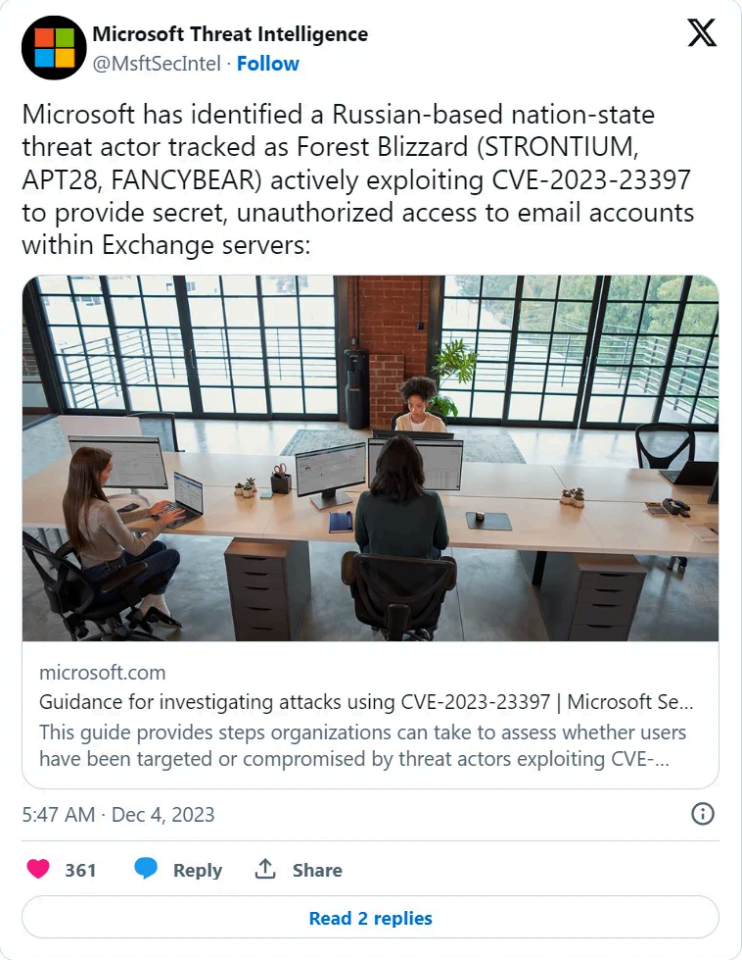
Microsoft's Threat Intelligence team issued a warning earlier today about the Russian state-sponsored actor APT28 (aka "Fancybear" or "Strontium") actively exploiting the CVE-2023-23397 Outlook flaw to hijack Microsoft Exchange accounts and steal sensitive information.

The targeted entities include government, energy, transportation, and other key organizations in the United States, Europe, and the Middle East.

The tech giant also highlighted the exploitation of other vulnerabilities with publicly available exploits in the same attacks, including CVE-2023-38831 in WinRAR and CVE-2021-40444 in Windows MSHTML.


F RTINET
0:00





Outlook flaw exploitation background

CVE-2023-23397 is a critical elevation of privilege (EoP) vulnerability in Outlook on Windows, which Microsoft fixed as a zero-day on the March 2023 Path Tuesday.

The disclosure of the flaw came with the revelation that APT28 had been exploiting it since April 2022 via specially crafted Outlook notes designed to steal NTLM hashes, forcing the target devices to authenticate to attacker-controlled SMB shares without requiring user interaction.

By elevating their privileges on the system, which was proven uncomplicated, APT28 performed lateral movement in the victim's environment and changed Outlook mailbox permissions to perform targeted email theft.

Despite the availability of security updates and mitigation recommendations, the attack surface remained significant, and a bypass of the fix (CVE-2023-29324) that followed in May worsened the situation.

Recorded Future warned in June that APT28 likely leveraged the Outlook flaw against key Ukrainian organizations. In October, the French cybersecurity agency (ANSSI) revealed that the Russian hackers had used the zero-click attack against government entities, businesses, universities, research institutes, and think tanks in France.

Attacks still ongoing

Microsoft's latest warning highlights that the GRU hackers still leverage CVE-2023-38831 in attacks, so there are still systems out there that remain vulnerable to the critical EoP flaw.

The tech firm has also noted the work of the Polish Cyber Command Center (DKWOC) in helping detect and stop the attacks. DKWOC also published a post describing APT28 activity that leverages CVE-2023-38831.

The recommended action to take right now, listed by priority, is the following:

- Apply the available security updates for CVE-2023-23397 and its bypass CVE-2023-29324.
- Use this script by Microsoft to check if any Exchange users have been targeted.
- Reset passwords of compromised users and enable MFA (multi-factor authentication) for all users.
- Limit SMB traffic by blocking connections to ports 135 and 445 from all inbound IP addresses
- Disable NTLM on your environment.

Given that APT28 is a highly resourceful and adaptive threat group, the most effective defense strategy is to reduce the attack surface across all interfaces and ensure all software products are regularly updated with the latest security patches.

Source: https://www.bleepingcomputer.com/news/microsoft/russian-hackers-exploiting-outlook-bug-to-hijack-exchange-accounts/