Microsoft Exchange servers hacked to deploy LockBit ransomware

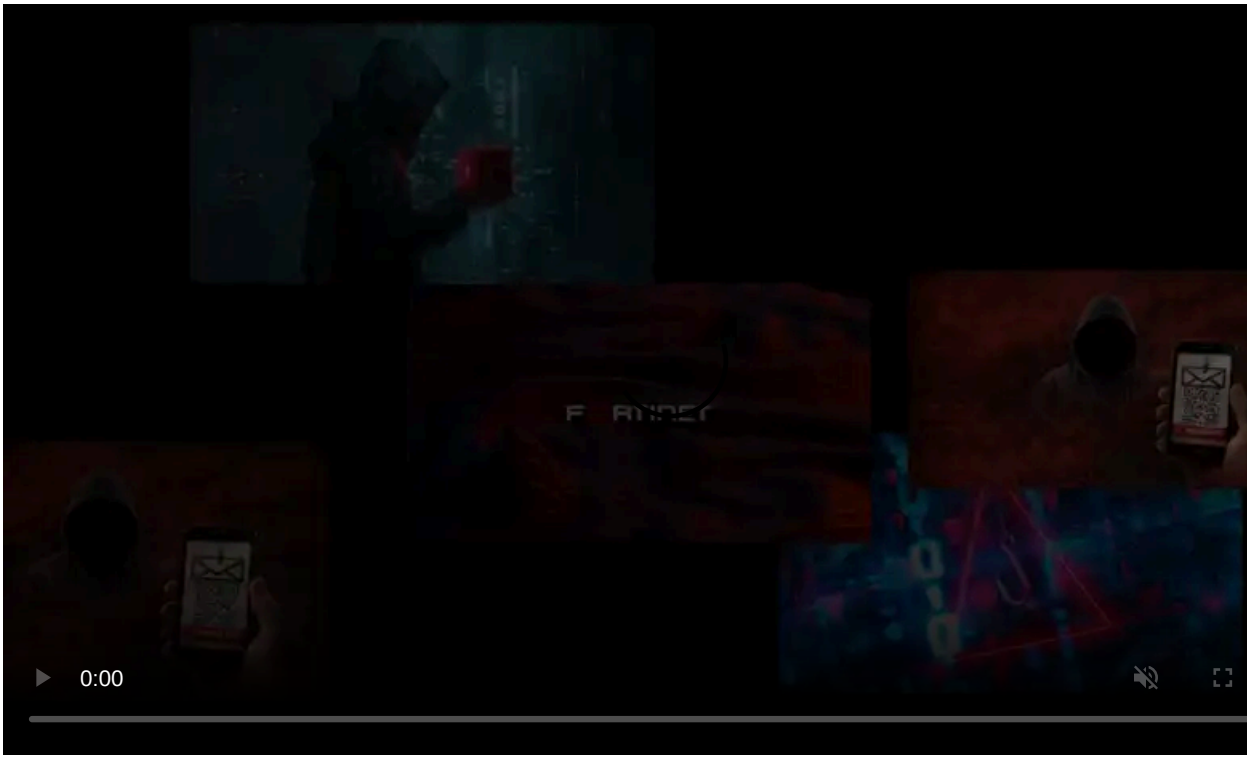
By Sergiu Gatlan

Published: 2022-10-11 · Archived: 2026-04-06 00:05:14 UTC

Microsoft is investigating reports of a new zero-day bug abused to hack Exchange servers which were later used to launch Lockbit ransomware attacks.

In at least one such incident from July 2022, the attackers used a previously deployed web shell on a compromised Exchange server to escalate privileges to Active Directory admin, steal roughly 1.3 TB of data, and encrypt network systems.

As described by South Korean cybersecurity firm AhnLab, whose forensic analysis experts were hired to help with the investigation, it took the threat actors only a week to hijack the AD admin account from when the web shell was uploaded.


0:00

AhnLab says the Exchange servers were likely hacked using an "undisclosed zero-day vulnerability," given that the victim received technical support from Microsoft to deploy quarterly security patches after a previous compromise from December 2021.

"Among the vulnerabilities disclosed after May, there were no reports of vulnerabilities related to remote commands or file creation," AhnLab explained.

"Therefore, considering that WebShell was created on July 21, it is expected that the attacker used an undisclosed zero-day vulnerability."

As a Microsoft spokesperson told BleepingComputer earlier today, the company is "investigating the claims in this report and will take any action needed to help protect customers."

New Microsoft Exchange zero-days?

While Microsoft is currently working on security patches to address two actively exploited Microsoft Exchange zero-days tracked as CVE-2022-41040 and CVE-2022-41082, AhnLab added that the one used to gain access to the Exchange server in July might be different since attack tactics don't overlap.

"There is a possibility that the vulnerabilities of Microsoft Exchange Server (CVE-2022-41040, CVE-2022-41082) disclosed by GTSC, a Vietnamese security company, on September 28 were used, but the attack method, the generated WebShell file name, and subsequent attacks after WebShell creation," AhnLab says.

"It is presumed that a different attacker used a different zero-day vulnerability."

Although differences in the delivery method can't be considered enough evidence the attackers used a new zero-day and security experts are also not convinced this is the case, at least one more security vendor knows of three other undisclosed Exchange flaws and provides "vaccines" to block exploitation attempts.

Discovered by Zero Day Initiative vulnerability researcher Piotr Bazydlo and reported to Microsoft three weeks ago, they are tracked by cybersecurity software firm Trend Micro tracks as ZDI-CAN-18881, ZDI-CAN-18882, and ZDI-CAN-18932 after its analysts validated the issues.

Undisclosed Exchange flaws (Trend Micro)

The company has also added detection signatures for these Exchange zero-days (tagged as critical severity by Trend Micro) to its IPS N-Platform, NX-Platform, or TPS products since October 4, 2022.

"This filter protects against exploitation of a zero-day vulnerability affecting Microsoft Exchange," Trend Micro says in a Digital Vaccine support document.

Microsoft hasn't disclosed any information regarding these three security flaws since they were reported and is yet to assign a CVE ID to track them.
