The Record.
Recorded Future® News

ZOHO

Catalin Cimpanu

September 8th, 2021

CISA warns of Zoho server zero-day exploited in the wild

The US Cybersecurity and Infrastructure Security Agency urged organizations today to apply the latest security update to their Zoho ManageEngine servers to patch a zero-day vulnerability that is currently being actively exploited in the wild for more than a week.

Tracked as CVE-2021-40539, the vulnerability impacts Zoho ManageEngine ADSelfService Plus, a password management and sign sign-on (SSO) solution from Indian company Zoho.

In a patch and security advisory published earlier today, Zoho described the zero-day as an authentication bypass that can be exploited via ADSelfService Plus REST API URLs and which could allow an attacker to execute malicious code on the underlying Zoho server.

"A remote attacker could exploit this vulnerability to take control of an affected system," CISA said today.

Zero-day exploited before last week's Confluence attacks

According to Matt Dahl, a Principal Intelligence Analyst at security firm CrowdStrike, the Zoho zero-day, while disclosed and patched today, has been under attack for more than a week, even before the attacks against Confluence servers that began last week.

In a series of tweets, Dahl described the attacks as targeted intrusions, most likely carried out by one threat actor.

"Actor(s) appeared to have a clear objective with ability to get in and get out quickly," Dahl said.

> *ManageEngine Exploit (CVE-2021-40539)*
>
> ** Limited use in targeted intrusion activity (Possibly a single actor, but unclear at this point)*
> ** Actor(s) appeared to have a clear objective with ability to get in and get out quickly*
> ** No known POC so exploit appears to be close-hold*
>
> *2/*
>
> — **Matt Dahl (@voodoodahl1)** September 8, 2021

No public exploit code or technical reports discussing the vulnerability are currently available, suggesting the threat actors discovered the bug on their own rather than weaponize public code.

How to detect exploitation

Companies and system administrators who'd like to investigate if their systems have been breached with this zero-day can follow the following steps, as laid out in the Zoho advisory linked above:

> In **\ManageEngine\ADSelfService Plus\logs** folder, search the access log entries for the strings listed below:
>
> 1. **/RestAPI/LogonCustomization**
>
> 2. **/RestAPI/Connection**

> If you find any of these two entries in the logs, it means your installation has been affected.

At the time of writing, there are more than 11,000 Zoho ManageEngine servers accessible over the internet.

This is the second major Zoho ManageEngine zero-day that has been actively exploited in attacks. The first, CVE-2020-10189, was exploited by cryptominers, ransomware gangs, and APT groups, and, according to the NSA, was one of the most commonly exploited vulnerabilities of 2020 used to plant web shells on servers.

● ● ● ● ●

News Technology

Tags India Vulnerability zero-day vulnerability disclosure

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

BRIEFS

Shopping scam sprawled across thousands of websites, bilked 'tens of millions of dollars' | October 31st, 2024

Russia to ban cryptocurrency mining in some regions due to electricity shortages | October 31st, 2024

Suspected pro-Ukraine cyberattack knocks out parking enforcement in Russian city | October 31st, 2024

UnitedHealth hires cybersecurity veteran as new CISO | October 30th, 2024

Texas county says 47,000 had SSNs, medical treatment info leaked during May cyberattack | October 28th, 2024

UK sanctions Russians over anti-Ukrainian disinformation campaigns | October 28th, 2024

EU president denounces Russian influence campaigns targeting Western Balkans | October 28th, 2024

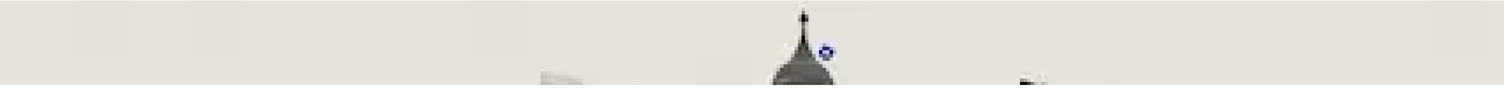
Free, France’s second-largest telecoms company, confirms being hit by cyberattack | October 28th, 2024

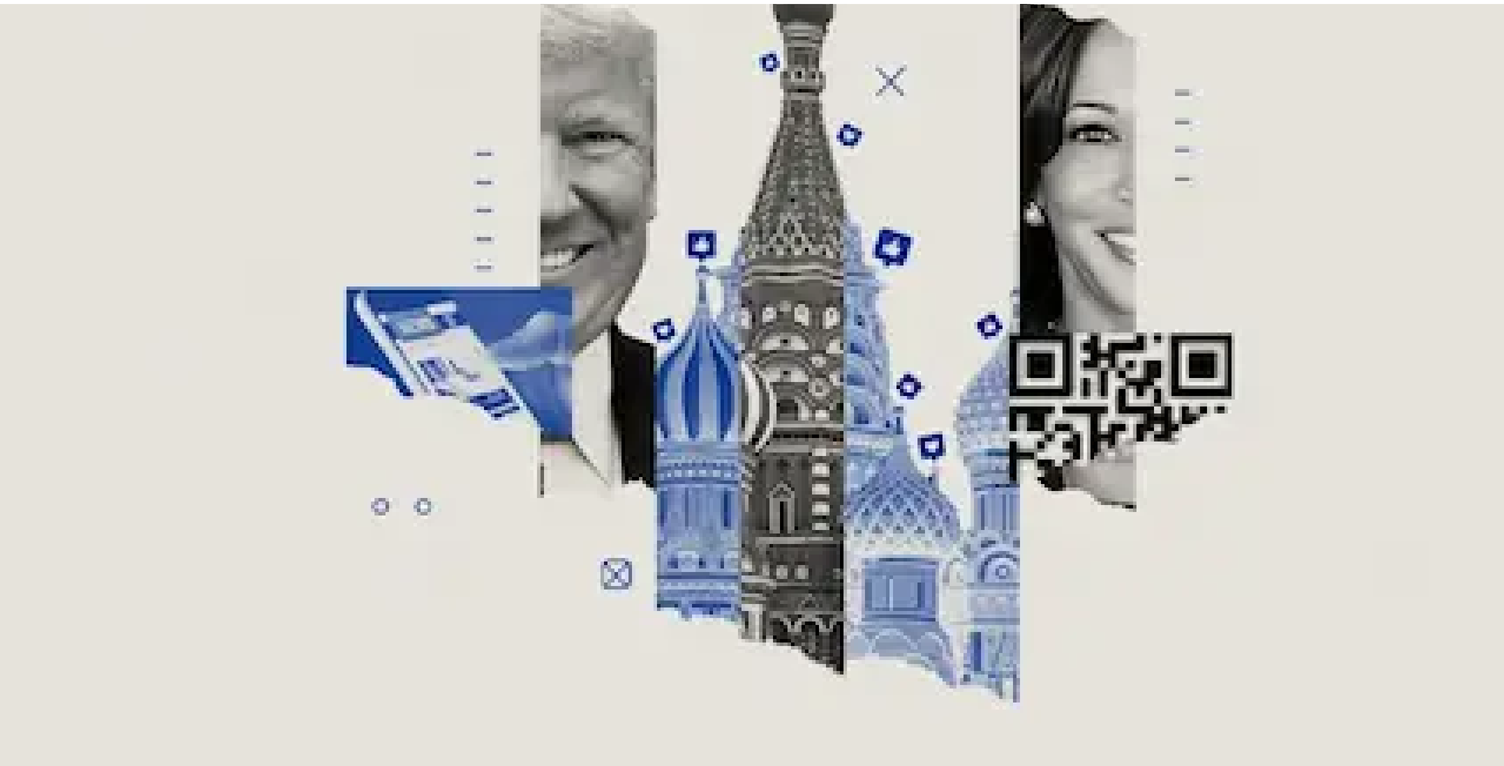
'All servers' for Redline and Meta infostealers hacked by Dutch police and FBI | October 28th, 2024

RUSSIAN STRATEGIC INFORMATION ATTACK FOR CATASTROPHIC EFFECT

RUSSIAN STRATEGIC INFORMATION ATTACK FOR CATASTROPHIC EFFECT

OPERATION OVERLOAD IMPERSONATES MEDIA TO INFLUENCE 2024 US ELECTION





OPERATION OVERLOAD IMPERSONATES MEDIA TO INFLUENCE 2024 US ELECTION

OUTMANEUVERING RHYSIDA: HOW ADVANCED THREAT INTELLIGENCE SHIELDS CRITICAL INFRASTRUCTURE FROM RANSOMWARE

OUTMANEUVERING RHYSIDA: HOW ADVANCED THREAT INTELLIGENCE SHIELDS CRITICAL INFRASTRUCTURE FROM RANSOMWARE

RHADAMANTHYS STEALER ADDS INNOVATIVE AI FEATURE IN VERSION 0.7.0

RHADAMANTHYS STEALER ADDS INNOVATIVE AI FEATURE IN VERSION 0.7.0

TARGETS, OBJECTIVES, AND EMERGING TACTICS OF POLITICAL DEEPFAKES

TARGETS, OBJECTIVES, AND EMERGING TACTICS OF POLITICAL DEEPFAKES

The Record.
Recorded Future® News

Privacy **About** **Contact Us**