Zoho patches actively exploited critical ADSelfService Plus bug

bleepingcomputer.com/news/security/zoho-patches-actively-exploited-critical-adselfservice-plus-bug/

Ionut Ilascu

By
Ionut Ilascu

- September 8, 2021
- 03:36 PM
- 0

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is warning that hackers are exploiting a critical vulnerability in Zoho's ManageEngine ADSelfService Plus password management solution that allows them to take control of the system.

ADSelfService Plus is aimed at larger organizations that need an integrated self-service password management for and single sign-on solution for Active Directory and cloud apps.

Exploits detected in the wild

The security issue is identified as CVE-2021-40539. It is considered critical as it can allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system.

Zoho has published a security advisory to announce that an update that patches the bug is currently available for ADSelfService Plus.

In a security notification week, the company says that it is “noticing indications of this vulnerability being exploited” in the wild.

The alert from CISA is clear about this, though, as the agency informs that “CVE-2021-40539 has been detected in exploits in the wild.”

At this moment, information about the vulnerability is scarce. A severity score has not been calculated by the National Institute of Standards and Technology in the U.S. but Zoho notes that the issue is critical:

“An authentication bypass vulnerability affecting REST API URLs, that could result in remote code execution,” the company says.

Organizations with ADSelfService Plus builds lower than 6114 are urged to apply the latest update from the developer, available using the service pack.

CVE-2021-40539 is the fifth critical vulnerability reported for Zoho ManageEngine ADSelfService Plus this year:

- CVE-2021-37421 - admin portal access-restriction bypass in Zoho ManageEngine ADSelfService Plus 6103 and earlier
- CVE-2021-37417 - CAPTCHA bypass due to improper parameter validation in Zoho ManageEngine ADSelfService Plus build 6103 and earlier
- CVE-2021-33055 - unauthenticated remote code execution in non-English editions affecting Zoho ManageEngine ADSelfService Plus through 6102
- CVE-2021-28958 - unauthenticated remote code execution while changing the password in all Zoho ManageEngine ADSelfService Plus builds up to 6101

Related Articles:

Zyxel fixes firewall flaws that could lead to hacked networks

Critical F5 BIG-IP vulnerability exploited to wipe devices

Mirai malware now delivered using Spring4Shell exploits

Exploit released for critical VMware auth bypass bug, patch now

Darknet market Versus shuts down after hacker leaks security flaw

- ADSelfService Plus
- CISA
- Critical Update

- Exploit
- ManageEngine
- Remote Code Execution
- Zoho

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

You may also like: