FBI and CISA warn of APT groups exploiting ADSelfService Plus

Posted: September 17, 2021 by Pieter Arntz

In a joint advisory the FBI, the United States Coast Guard Cyber Command (CGCYBER), and the Cybersecurity and Infrastructure Security Agency (CISA) warn that advanced persistent threat (APT) cyber-actors may be exploiting a vulnerability in ManageEngine's single sign-on (SSO) solution.

The vulnerability

Publicly disclosed computer security flaws are listed in the Common Vulnerabilities and Exposures (CVE) database. Its goal is to make it easier to share data across separate vulnerability capabilities (tools, databases, and services). The vulnerability in questions is listed under CVE-2021-40539 as a REST API authentication bypass with resultant remote code execution (RCE) in Zoho ManageEngine ADSelfService Plus version 6113 and prior.

The vulnerability allows an attacker to gain unauthorized access to the product through REST API endpoints by sending a specially crafted request. This would allows attackers to carry out subsequent attacks resulting in RCE.

For those that have never heard of this software, it's a self-service password management and single sign-on (SSO) solution for Active Directory (AD) and cloud apps. Which means that any attacker that is able to exploit this vulnerability immediately has access to some of the most critical parts of a corporate network.

In-the-wild exploitation

When word of the vulnerability came out it was already clear that is was being exploited in the wild. Zoho remarked that it was noticing indications of this vulnerability being exploited. Other researchers chimed in saying the attacks had thus far been highly targeted and limited, and possibly the work of a single threat-actor. Yesterday's joint advisory seems to support that, telling us that APT cyber-actors are likely among those exploiting the vulnerability.

They find this of high concern since this poses a serious risk to critical infrastructure companies. CISA recognizes 16 critical infrastructure sectors whose "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."

The joint advisory points out that the suspected APT cyber-actors have targeted academic institutions, defense contractors, and critical infrastructure entities in multiple industry sectors—including transportation, IT, manufacturing, communications, logistics, and finance.

It also warns that successful exploitation of the vulnerability allows an attacker to place web shells, which enable the adversary to conduct post-exploitation activities, such as compromising administrator credentials, conducting lateral movement, and exfiltrating registry hives and Active Directory files.

According to the advisory, the JavaServer Pages web shell arrives as a `.zip` file "masquerading as an x509 certificate" called `service.cer`. The web shell is then accessed via the URL path `/help/admin-guide/Reports/ReportGenerate.jsp`.

However, it warns:

> Confirming a successful compromise of ManageEngine ADSelfService Plus may be difficult—the attackers run clean-up scripts designed to remove traces of the initial point of compromise and hide any relationship between exploitation of the vulnerability and the web shell.

Please consult the advisory for a full list of IOCs.

Mitigation

A patch for this vulnerability was made available on September 7, 2021. Users are advised to update to ADSelfService Plus build 6114. The FBI, CISA, and CGCYBER also strongly urge organizations to make sure that ADSelfService Plus is not directly accessible from the Internet.

The ManageEngine site has specific instructions on how to identify and update vulnerable installations. It also has information about how you can reach out to support if you need further information, have any

questions, or face any difficulties updating ADSelfService Plus.

Stay safe, everyone!

Related

500,000 Fortinet VPN credentials exposed: Turn off, patch, reset passwords
September 9, 2021
In "Exploits and vulnerabilities"

[updated] Patch now! PrintNightmare over, MSHTML fixed, a new horror appears ... OMIGOD
September 15, 2021
In "Exploits and vulnerabilities"

BrakTooth Bluetooth vulnerabilities, crash all the devices!
September 2, 2021
In "Exploits and vulnerabilities"

SHARE THIS ARTICLE

COMMENTS

RELATED ARTICLES

ABOUT THE AUTHOR

Pieter Arntz
Malware Intelligence Researcher

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.

CAREERS (https://jobs.malwarebytes.com/)

NEWS AND PRESS (https://press.malwarebytes.com/)

MY ACCOUNT

SIGN IN (https://my.malwarebytes.com/en/login)

CONTACT US

GET SUPPORT (https://support.malwarebytes.com/hc/en-us)

CONTACT SALES (https://www.malwarebytes.com/contact/)

3979 Freedom Circle, 12th Floor
Santa Clara, CA 95054

(https://twitter.com/malwarebytes) (https://www.facebook.com/malwarebytes/) (https://www.linkedin.com/company/malwarebytes) (https://www.youtube.com/user/malwarebytes1) (https://www.instagram.com/malwarebytes/)

ENGLISH

Legal (//www.malwarebytes.com/legal/) Privacy (//www.malwarebytes.com/legal/privacy-policy) Accessibility (//www.malwarebytes.com/accessibility/) Terms of Service (//www.malwarebytes.com/tos/)