LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Sector Alert

November 12, 2021 TLP: WHITE Report: 202111121500

Chinese Cyberespionage Campaign Targets Multiple Industries Including Healthcare by Exploiting Critical Vulnerability in Password Management Product

Executive Summary

Multiple cybersecurity organizations recently shared information regarding a suspected Chinese cyberespionage campaign targeting organizations in multiple industries, including healthcare, by exploiting a critical vulnerability in a common password management product. This activity began as early as September 17, 2021, and there are patches, mitigations, and workarounds available to detect and mitigate this threat.

Report

On November 7, 2021, researchers at Palo Alto Networks Unit 42 shared details of a targeted attack campaign beginning around September 17, 2021, with scans against vulnerable Zoho ManageEngine ADSelfService Plus servers. After gaining initial access, the attackers attempt to deliver multiple malware families, including Godzilla webshells, NGLite trojan, and the KdcSponge information stealer. ManageEngine ADSelfService Plus is an integrated self-service password management and single sign-on solution for Active Directory and cloud apps. The researchers stated that the campaign has already resulted in the compromise of at least nine organizations worldwide from critical sectors including healthcare. Initial attribution analysis conducted by Unit 42 indicated that APT27 was behind this cyber espionage campaign which exploits a critical vulnerability (CVE-2021-40539) in ManageEngine. The researchers believe that the group targeted at least 370 Zoho ManageEngine servers in the United States alone and there are over 11,000 internet-exposed servers running the vulnerable Zoho software.

APT27 is a Chinese threat group that is also known by various private cybersecurity industry partners as TG-3390, Emissary Panda, BRONZE UNION, Iron Tiger, and LuckyMouse. APT27 engages in cyber operations where the goal is intellectual property theft, usually focusing on the data that make a particular organization competitive within its field. APT27 threat actors are not known for using original zero-day exploits, but they may leverage those exploits once they have been made public, as in this case, with exploitation attempts beginning about 10 days later.

The next day, on November 8, 2021, the Microsoft Threat Intelligence Center (MSTIC) shared additional information related to this threat activity, attributing the campaign with high confidence to DEV-0322, the temporary designation for a threat group operating out of China, based on observed infrastructure, victimology, tactics, and procedures. MSTIC first observed the latest DEV-0322 campaign on September 22, 2021, with activity against targets that appear to be in the Defense Industrial Base, higher education, consulting services, and information technology sectors. Following initial exploitation of CVE-2021-40539 on a targeted system, DEV-0322 performed several activities including credential dumping, installing custom binaries, and dropping malware to maintain persistence and move laterally within the network.

Analysis

Based on available open source information regarding this threat activity, HC3 assesses with high confidence that the goal of this campaign is to conduct strategic intellectual property theft from targets in a wide range of industries, including healthcare, by stealing credentials, establishing persistence, and gathering sensitive files from victims. It is also highly likely that other state-backed or financially-motivated threat actors are exploiting this vulnerability.

Vulnerabilities

CVE-ID	CVE Description
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus version 6113 and prior is vulnerable to REST API authentication bypass with resultant remote code execution. This vulnerability has received a Critical severity rating.

Patches, Mitigations, and Workarounds

Patches for this critical authentication bypass vulnerability were issued on September 7, 2021, and on September 16, 2021. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) released an alert warning that the flaw was being actively exploited by advanced persistent threat (APT) actors. This vulnerability can be mitigated by updating to ADSelfService Plus build 6114.

According to the affected product vendor, there are also three ways to check if your installation is impacted:

1. Run the ManageEngine exploit detection tool.
2. Check for specific log entries.
3. Check for specific files in your system.

CISA has provided additional technical information, including associated Mitre ATT&CK techniques, indicators of compromise, and mitigations, in its September 16 joint advisory, Alert (AA21-259A).

References

"Advanced Persistent Threat Groups: APT27," Mandiant. https://www.mandiant.com/resources/apt-groups

"Alert (AA21-259A) APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus," CISA. September 16, 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-259a

"CVE-2021-40539," Mitre. September 06, 2021. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40539

Dark Reading Staff. "FBI, CISA, CGCYBER Warn of APTs Targeting CVE-2021-40539," Dark Reading. September 16, 2021. https://www.darkreading.com/threat-intelligence/fbi-cisa-cgcyber-warn-of-apts-targeting-cve-2021-40539

Falcone, Robert, Jeff White, and Peter Renals. "Targeted Attack Campaign Against ManageEngine ADSelfService Plus Delivers Godzilla Webshells, NGLite Trojan and KdcSponge Stealer," Palo Alto. November 7, 2021. https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/

Gatlan, Sergiu. "State hackers breach defense, energy, healthcare orgs worldwide," Bleeping Computer. November 8, 2021. https://www.bleepingcomputer.com/news/security/state-hackers-breach-defense-energy-healthcare-orgs-worldwide/

Microsoft Threat Intelligence Center. "Threat actor DEV-0322 exploiting ZOHO ManageEngine ADSelfService Plus," Microsoft. November 8, 2021. https://www.microsoft.com/security/blog/2021/11/08/threat-actor-dev-0322-exploiting-zoho-manageengine-adselfservice-plus/

O'Donnell-Welch, Lindsey. "Attackers Exploit ManageEngine Flaw To Steal Sensitive Data," Duo. November 8, 2021. https://duo.com/decipher/attackers-exploit-manageengine-flaw-to-breach-nine-organizations

“Security advisory - ADSelfService Plus authentication bypass vulnerability,” ManageEngine. https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html

“Threat Group-3390,” Mitre ATT&CK. October 12, 2021. https://attack.mitre.org/groups/G0027/

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback