JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:AMBER

Product ID: AA21-250A

September 7, 2021

APT Actors Exploiting Newly Identified CVE-2021-40539 in ManageEngine ADSelfService Plus

This Joint Cybersecurity Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 8. See the ATT&CK for Enterprise framework for referenced threat actor techniques and for mitigations.

SUMMARY

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), United States Coast Guard Cyber Command (CGCYBER), and the Cybersecurity and Infrastructure Security Agency (CISA) to highlight the cyber threat associated with active exploitation of a newly identified vulnerability (CVE-2021-40539) in ManageEngine ADSelfService Plus—a self-service password management and single sign-on solution.

CVE-2021-40539, rated critical, is an authentication bypass vulnerability affecting REST API URLs that could enable remote code execution. The FBI and CISA assess that advanced persistent threat (APT) cyber actors are likely among those exploiting the vulnerability. The exploitation of ManageEngine ADSelfService Plus poses a serious risk to critical infrastructure companies, U.S.-cleared defense contractors, academic institutions, and other entities that use the software. Successful exploitation of the vulnerability allows an attacker to place webshells, 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.

New Zoho ManageEngine ADSelfService Plus build 6114 fixes CVE-2021-40539. ManageEngine announced the security vulnerability on September 6, 2021 and advised customers to patch immediately. Additional information can be found at:

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at https://www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov**. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. **To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov. To contact Coast Guard Cyber Command in relation to this, please email maritimecyber@uscg.mil.

https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release.

The FBI and CISA have reports of malicious cyber actors using exploits against CVE-2021-40539 to gain access [T1190] to ManageEngine ADSelfService Plus, as early as August 2021. Various tactics, techniques, and procedures (TTPs) have been identified, but the actor(s) frequently appeared to be writing webshells [T1505.003] to disk for initial persistence, utilizing custom obfuscation for command and control protocols (C2) [T1027 and T1140], conducting further operations to dump user credentials [T1003], living off the land by only using signed Windows binaries for follow-on actions [T1218], adding/deleting user accounts as needed [T1136], and stealing copies of the Active Directory database (`NTDS.dit`) [T1003.003] or registry hives. This information has been shared with multiple other U.S. Government (USG) agencies.

The FBI is proactively investigating this malicious cyber activity, leveraging specially trained cyber squads in each of its 56 field offices and CyWatch, the FBI's 24/7 operations center and watch floor, which provides around-the-clock support to track incidents and communicate with field offices across the country and partner agencies. Sharing technical and/or qualitative information with the FBI and CISA helps empower and amplify our capabilities as federal partners to collect and share intelligence and engage with victims while working to unmask and hold accountable, those conducting malicious cyber activities. CGCYBER has deployable elements that provide cyber capability to marine transportation system critical infrastructure in proactive defense or response to incidents.

TECHNICAL DETAILS

Compromise of the affected systems involves exploitation of CVE-2021-40539 in ADSelfService Plus, allowing the attacker to upload a `.zip` file containing a webshell masquerading as an x509 certificate: `service.cer`. Subsequent requests are then made to different API endpoints to further exploit the system.

After the initial exploitation, the JSP webshell is accessible at `/help/admin-guide/Reports/ReportGenerate.jsp`. The attacker then attempts to move laterally using Windows Management Instrumentation (WMI), gain access to a domain controller, dump `NTDS.dit` and `SECURITY/SYSTEM` registry hives, and then, from there, continues the compromised access.

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 webshell.

Targeted Sectors

APT cyber actors have targeted academic institutions, defense contractors, and critical infrastructure entities in multiple industry sectors including transportation, information technology (IT), manufacturing, communications, logistics, and finance. Illicitly obtained access and information may disrupt company operations and subvert U.S. research in multiple sectors.

Indicators of Compromise:

Hashes:

`068d1b3813489e41116867729504c40019ff2b1fe32aab4716d429780e666324`

`49a6f77d380512b274baff4f78783f54cb962e2a8a5e238a453058a351fcfbba`

Filepaths:

```
C:\ManageEngine\ADSelfService Plus\webapps\adssp\help\admin-guide\reports\ReportGenerate.jsp
C:\ManageEngine\ADSelfService Plus\webapps\adssp\html\promotion\adap.jsp
C:\ManageEngine\ADSelfService Plus\work\Catalina\localhost\ROOT\org\apache\jsp\help
C:\ManageEngine\ADSelfService Plus\jre\bin\SelfSe~1.key (filename varies with an epoch timestamp of creation, extension may vary as well)
C:\ManageEngine\ADSelfService Plus\webapps\adssp\Certificates\SelfService.csr
C:\ManageEngine\ADSelfService Plus\bin\service.cer
C:\Users\Public\custom.txt
C:\Users\Public\custom.bat
C:\ManageEngine\ADSelfService Plus\work\Catalina\localhost\ROOT\org\apache\jsp\help (including subdirectories and contained files)
```

Webshell URL Paths:

`/help/admin-guide/Reports/ReportGenerate.jsp`

`/html/promotion/adap.jsp`

Check logfiles located at `C:\ManageEngine\ADSelfService Plus\logs` for evidence of successful exploitation of the ADSelfService Plus vulnerability:

- In access* logs:
  - `/help/admin-guide/Reports/ReportGenerate.jsp`
  - `/ServletApi/../RestApi/LogonCustomization`
  - `/ServletApi/../RestAPI/Connection`
- In serverOut_* logs:
  - `Keystore will be created for "admin"`
  - `The status of keystore creation is Upload!`
- In adslog* logs:
  - Java traceback errors that include references to NullPointerException in `addSmartCardConfig` or `getSmartCardConfig`

TTPs:

- WMI for lateral movement and remote code execution (`wmic.exe`)
- Using plaintext credentials acquired from compromised ADSelfService Plus host

- Using `pg_dump.exe` to dump ManageEngine databases
- Dumping `NTDS.dit` and `SECURITY/SYSTEM/NTUSER` registry hives
- Exfiltration through webshells
- Post-exploitation activity conducted with compromised U.S. infrastructure
- Deleting specific, filtered log lines

Yara Rules:

```
rule ReportGenerate_jsp {
   strings:
      $s1 = "decrypt(fpath)"
      $s2 = "decrypt(fcontext)"
      $s3 = "decrypt(commandEnc)"
      $s4 = "upload failed!"
      $s5 = "sevck"
      $s6 = "newid"
   condition:
      filesize < 15KB and 4 of them
}

rule EncryptJSP {
   strings:
      $s1 = "AEScrypt"
      $s2 = "AES/CBC/PKCS5Padding"
      $s3 = "SecretKeySpec"
      $s4 = "FileOutputStream"
      $s5 = "getParameter"
      $s6 = "new ProcessBuilder"
      $s7 = "new BufferedReader"
      $s8 = "readLine()"
   condition:
      filesize < 15KB and 6 of them
}
```

MITIGATIONS

Compromise Mitigations

Organizations that identify any activity related to ManageEngine ADSelfService Plus indicators of compromise within their networks should take action immediately.

New Zoho ManageEngine ADSelfService Plus build 6114 fixes CVE-2021-40539. ManageEngine announced the security vulnerability on September 6, 2021, and advised customers patch immediately. Additional information can be found at: https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release.

FBI and CISA also strongly recommend domain-wide password resets and double Kerberos TGT password resets if any indication is found that the `NTDS.dit` file was compromised.

Actions for Affected Organizations

Immediately report as an incident to **CISA** or the **FBI** (refer to Contact information section below) the existence of any of the following:

- Identification of indicators of compromise as outlined above.
- Presence of webshell code on compromised ManageEngine ADSelfService Plus servers.
- Unauthorized access to or use of accounts.
- Evidence of lateral movement by malicious actors with access to compromised systems.
- Other indicators of unauthorized access or compromise.

CONTACT INFORMATION

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- The FBI through the FBI Cyber Division (855-292-3937 or CyWatch@fbi.gov) or a local field office,
- CISA (888-282-0870 or Central@cisa.dhs.gov).

To report Cyber incidents to the U.S. Coast Guard, please contact the USCG National Response Center (NRC) Phone: 1-800-424-8802, email: NRC@uscg.mil.