JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-259A

September 16, 2021

APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus

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.

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.

CVE-2021-40539, rated critical by the Common Vulnerability Scoring System (CVSS), is an authentication bypass vulnerability affecting representational state transfer (REST) application programming interface (API) URLs that could enable remote code execution. The FBI, CISA, and CGCYBER 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.

Zoho ManageEngine ADSelfService Plus build 6114, which Zoho released on September 6, 2021, fixes CVE-2021-40539. FBI, CISA, and CGCYBER strongly urge users and administrators to update to ADSelfService Plus build 6114. Additionally, FBI, CISA, and CGCYBER strongly urge organizations ensure ADSelfService Plus is not directly accessible from the internet.

The FBI, CISA, and CGCYBER 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. The actors have been observed using various tactics, techniques, and procedures (TTPs), including:

- Frequently writing webshells [T1505.003] to disk for initial persistence
- Obfuscating and Deobfuscating/Decoding Files or Information [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]
- Stealing copies of the Active Directory database (`NTDS.dit`) [T1003.003] or registry hives
- Using Windows Management Instrumentation (WMI) for remote execution [T1047]
- Deleting files to remove indicators from the host [T1070.004]
- Discovering domain accounts with the `net` Windows command [1087.002]
- Using Windows utilities to collect and archive files for exfiltration [T1560.001]
- Using custom symmetric encryption for command and control (C2) [T1573.001]

The FBI, CISA, and CGCYBER are proactively investigating and responding to this malicious cyber activity.

- FBI is 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.
- CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.
- CGCYBER has deployable elements that provide cyber capability to marine transportation system critical infrastructure in proactive defense or response to incidents.

Sharing technical and/or qualitative information with the FBI, CISA, and CGCYBER 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.

TECHNICAL DETAILS

Successful compromise of ManageEngine ADSelfService Plus, via exploitation of CVE-2021-40539, allows the attacker to upload a `.zip` file containing a JavaServer Pages (JSP) webshell masquerading as an x509 certificate: `service.cer`. Subsequent requests are then made to different API endpoints to further exploit the victim's 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, 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`

File paths:

```
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 log files 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

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

Zoho ManageEngine ADSelfService Plus build 6114, which Zoho released on September 6, 2021, fixes CVE-2021-40539. FBI, CISA, and CGCYBER strongly urge users and administrators to update

to ADSelfService Plus build 6114. Additionally, FBI, CISA, and CGCYBER strongly urge organizations ensure ADSelfService Plus is not directly accessible from the internet.

Additionally, FBI, CISA, and CGCYBER strongly recommend domain-wide password resets and double Kerberos Ticket Granting Ticket (TGT) password resets if any indication is found that the `NTDS.dit` file was compromised.