Hive Pro

# THREAT ADVISORY

## ManageEngine ADSelfService Plus has been abused in the wild due to a zero-day vulnerability

**TA202134**

**Threat Level** RED

**Publish Date –** Sept 19, 2021

An APT actor is attempting to exploit a zero-day vulnerability in ManageEngine ADSelfService Plus, a self-service password management and single sign-on solution that poses a high risk to critical infrastructure companies, US-cleared defense contractors, academic institutions, and other entities that use the software. The FBI, CISA, and CGCYBER highly advise companies to ensure that ADSelfService Plus is not directly accessible via the internet. The Hive pro threat research team also recommends that ADSelfService be updated to version 6114.

The techniques used by the APT actor includes:

- T1190 - Exploit Public-Facing Application
- T1505.003 - Server Software Component: Web Shell
- T1027- Obfuscated Files or Information
- T1140 - Deobfuscate/Decode Files or Information
- T1003 - OS Credential Dumping
- T1218 - Signed Binary Proxy Execution
- T1136 - Create Account
- T1003.003 - OS Credential Dumping: NTDS
- T1047 - Windows Management Instrumentation
- T1070.004 - Indicator Removal on Host: File Deletion
- T1087.002 - Account Discovery: Domain Account
- T1560.001 - Archive Collected Data: Archive via Utility
- T1573.001 - Encrypted Channel: Symmetric Cryptography

### Vulnerability Details

| CVE ID | Affected Versions | Affected CPE | Vulnerability Name | CWE ID |
|---|---|---|---|---|
| CVE-2021-40539 | Zoho ManageEngine ADSelfService Plus up to 6.1:6113 | cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:4.5:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.0:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.1:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.2:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.3:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.4:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.5:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.6:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.7:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.8:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:6.0:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:6.1:*:*:*:*:*:*:* | Zoho ManageEngine ADSelfService Plus REST API improper authentication | CWE-287 |

## Indicators of Compromise (IoCs)

| Type | Value |
|---|---|
| SHA-2 Hash | 49A6F77D380512B274BAFF4F78783F54CB962E2A8A5E238A453058A351FCFBBA<br>068D1B3813489E41116867729504C40019FF2B1FE32AAB4716D429780E666324 |
| File Paths | C:\ManageEngine\ADSelfService Plus\webapps\adssp\help\admin-guide\reports\ReportGenerate.jsp<br>C:\ManageEngine\ADSelfService Plus\webapps\adssp\html\promotion\adap.jsp<br>C:\ManageEngine\ADSelfService Plus\work\Catalina\localhost\ROOT\org\apache\jsp\help<br>C:\ManageEngine\ADSelfService Plus\jre\bin\SelfSe~1.key (filename varies with an epoch timestamp of creation, extension may vary as well)<br>C:\ManageEngine\ADSelfService Plus\webapps\adssp\Certificates\SelfService.csr<br>C:\ManageEngine\ADSelfService Plus\bin\service.cer<br>C:\Users\Public\custom.txt<br>C:\Users\Public\custom.bat<br>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<br>/html/promotion/adap.jsp |

## Patch Link

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

## References

https://us-cert.cisa.gov/ncas/alerts/aa21-259a