

ManageEngine ADSelfService Plus 6000 Remote Code Execution

Authored by Bhadresh Patel

Posted Aug 10, 2020

ManageEngine ADSelfService Plus 6000 unauthenticated remote code execution exploit.

tags | exploit, remote, code execution

advisories | CVE-2020-11552

SHA-256 | fa384c7e23223ad88e958b30f63828edb593906fd8b96943cad069ac163c70e2 Download | Favorite | View

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

# Exploit Title: ManageEngine ADSelfService Plus 6000 - Unauthenticated Remote Code Execution  
# Date: 2020-08-08  
# Exploit Author: Bhadresh Patel  
# Vendor link: https://www.manageengine.com/company.html  
# Version: ADSelfService Plus build < 6003  
# CVE : CVE-2020-11552

This is an article with PoC exploit video of ManageEngine ADSelfService Plus - Unauthenticated Remote Code Execution Vulnerability

Title:

ManageEngine ADSelfService Plus - Unauthenticated Remote Code Execution Vulnerability

CVE ID:

CVE-2020-11552

Date:

08/08/2020 (dd/mm/yyyy)

Vendor:

As the IT management division of Zoho Corporation, ManageEngine prioritizes flexible solutions that work for all businesses, regardless of size or budget.

ManageEngine crafts comprehensive IT management software with a focus on making your job easier. Our 90+ products and free tools cover everything your IT needs, at prices you can afford.

From network and device management to security and service desk software, we're bringing IT together for an integrated, overarching approach to optimize your IT.

Vendor link: https://www.manageengine.com/company.html

Vulnerable Product:

ManageEngine ADSelfService Plus is an integrated self-service password management and single sign on solution. This solution helps domain users perform self-service password reset, self-service account unlock, employee self-update of personal details (e.g., mobile numbers and photos) in Microsoft Windows Active Directory. ADSelfService Plus also provides users with secure, one-click access to all SAML-supported enterprise applications, including Office 365, Salesforce, and G Suite, through Active Directory-based single sign-on (SSO). For improved security, ADSelfService Plus offers Windows two-factor authentication for all remote and local logins. Administrators find it easy to automate password resets, account unlocks while optimizing IT expenses associated with help desk calls.

Product link:

https://www.manageengine.com/products/self-service-password/?meadsol

Abstract:

A remote code execution vulnerability exists in ManageEngine ADSelfService Plus Software when it does not properly enforce user privileges associated with Windows Certificate Dialog. This vulnerability could allow an unauthenticated attacker to remotely execute commands with system level privileges on target windows host. An attacker does not require any privilege on the target system in order to exploit this vulnerability.

Report-Timeline:

27/02/2020: Vendor notified  
27/02/2020: Vendor response  
28/02/2020: Marked duplicate  
11/03/2020: Patch released  
23/03/2020: Vendor responded regarding patch release update  
26/03/2020: Patch tested and found that it partially fixed the issue. Reported back to the vendor.  
18/04/2020: Shared updated report with new PoC  
22/04/2020: Vendor acknowledged the issue  
24/07/2020: Patch released ( https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6003-release-faceid-support )  
08/08/2020: Public disclosure

Affected Software Version:

< ADSelfService Plus build 6003

Exploitation-Technique:

Remote

Severity Rating (CVSS):

9.8 (Critical) (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Details:

A remote code execution vulnerability exists in ManageEngine ADSelfService Plus Software when it does not properly enforce user privileges associated with Windows Certificate Dialog.

This vulnerability could allow an unauthenticated attacker to remotely execute commands with system level privileges on target windows host. An attacker does not require any privilege on the target system in order to exploit this vulnerability.

ManageEngine ADSelfService Plus thick client enables a user to perform self-service like password reset, self-service account unlock, etc by using self-service option on windows login screen.

Upon selecting this option, ManageEngine ADSelfService Plus thick client software will be launched which will connect to a remote ADSelfServicePlus server to facilitate the self-service operations.

A security alert can/will be triggered when "an unauthenticated attacker having physical access to the host issues a self-signed SSL certificate to the client". Or, "a (default) self-signed SSL certificate is configured on ADSelfService Plus server".

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 154 files

Ubuntu 73 files

LiquidWorm 23 files

Debian 18 files

malvuln 11 files

nu11security 11 files

Gentoo 9 files

Google Security Research 8 files

T. Weber 4 files

Julien Ahrens 4 files

File Tags

ActiveX (932)  
Advisory (79,754)  
Arbitrary (15,694)  
BBS (2,859)  
Bypass (1,619)  
CGI (1,018)  
Code Execution (8,926)  
Conference (673)  
Cracker (840)  
CSRF (3,290)  
DoS (22,602)  
Encryption (2,349)  
Exploit (50,359)  
File Inclusion (4,165)  
File Upload (946)  
Firewall (821)  
Info Disclosure (2,660)  
Intrusion Detection (867)  
Java (2,899)  
JavaScript (821)  
Kernel (6,291)  
Local (14,201)  
Magazine (586)  
Overflow (12,419)  
Perl (1,418)  
PHP (5,093)  
Proof of Concept (2,291)  
Protocol (3,435)  
Python (1,467)  
Remote (30,044)  
Root (3,504)  
Ruby (594)  
Scanner (1,631)  
Security Tool (7,777)  
Shell (3,103)  
Shellcode (1,204)  
Sniffer (886)

File Archives

December 2022  
November 2022  
October 2022  
September 2022  
August 2022  
July 2022  
June 2022  
May 2022  
April 2022  
March 2022  
February 2022  
January 2022  
Older

Systems

AIX (426)  
Apple (1,926)  
BSD (370)  
CentOS (55)  
Cisco (1,917)  
Debian (6,634)  
Fedora (1,690)  
FreeBSD (1,242)  
Gentoo (4,272)  
HPUX (878)  
IOS (330)  
iPhone (108)  
IRIX (220)  
Juniper (67)  
Linux (44,315)  
Mac OS X (684)  
Mandriva (3,105)  
NetBSD (255)  
OpenBSD (479)  
RedHat (12,469)  
Slackware (941)  
Solaris (1,607)

```
"View Certificate" option from the security alert will allow an attacker
with physical access or a remote attacker with RDP access, to export a
displayed certificate to a file. This will further cascade to the standard
dialog/wizard which will open file explorer as SYSTEM.

By navigating file explorer through "C:\windows\system32\", a cmd.exe can
be launched as a SYSTEM.

*PoC Video:* https://www.youtube.com/watch?v=sl2RXffswnQ

01:00 to 05:30 : Setup the environment
05:30 to 06:34 : Exploitation

Credits:
=====
Bhadresh Patel

-----
Regards,
-Bhadresh
```

- [Spoof](#) (2,166)
- [SQL Injection](#) (16,102)
- [TCP](#) (2,379)
- [Trojan](#) (686)
- [UDP](#) (676)
- [Virus](#) (662)
- [Vulnerability](#) (31,136)
- [Web](#) (9,365)
- [Whitepaper](#) (3,729)
- [x86](#) (946)
- [XSS](#) (17,494)
- [Other](#)
- [SUSE](#) (1,444)
- [Ubuntu](#) (8,199)
- [UNIX](#) (9,159)
- [UnixWare](#) (185)
- [Windows](#) (6,511)
- [Other](#)

[Login](#) or [Register](#) to add favorites

Site Links


- [News by Month](#)
- [News Tags](#)
- [Files by Month](#)
- [File Tags](#)
- [File Directory](#)


About Us

- [History & Purpose](#)
- [Contact Information](#)
- [Terms of Service](#)
- [Privacy Statement](#)
- [Copyright Information](#)

Hosting By

- [Rokasec](#)

 Follow us on Twitter

 Subscribe to an RSS Feed