ManageEngine ADSelfService Plus – Unauthenticated Remote Code Execution Vulnerability

From: Bhdresh <bhdresh () gmail com>
Date: Sat, 8 Aug 2020 03:52:49 +0400

```
Hello,

Please find the below vulnerability details,

-----------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------

# Exploit Title: ManageEngine ADSelfService Plus - Unauthenticated Remote
Code Execution Vulnerability
# Date: 08/08/2020
# Exploit Author: Bhadresh Patel
# 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:
====
ManageEngineADSelfService Plus - UnauthenticatedRemote Code Execution
Vulnerability

CVE ID:
=======

CVE-2020-11552

Date:
====
08/08/2020 (dd/mm/yyyy)

Vendor:
======
As the IT management division of Zoho Corporation, ManageEngineprioritizes
flexible solutions that work for all businesses,regardless of size or
budget.

ManageEnginecrafts 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.

Vendorlink: https://www.manageengine.com/company.html


Vulnerable Product:
==============
ManageEngineADSelfService 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)
inMicrosoft 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,throughActive
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.

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

Abstract:
=======
A remote code execution vulnerability exists in ManageEngineADSelfService
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


AffectedSoftware Version:
=============
< ADSelfService Plus build 6003

Exploitation-Technique:
===================
Remote and Physical both

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 ManageEngineADSelfService
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.

ManageEngineADSelfService 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 SSLcertificate to the client". Or, "a (default) self-signed SSLcertificate is configured on ADSelfService Plus server".

"ViewCertificate" 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\", acmd.exe can be launched as a SYSTEM.

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

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

Credits:
=======
BhadreshPatel

Regards,
-Bhadresh

By Date By Thread

Current thread:

- **ManageEngine ADSelfService Plus – Unauthenticated Remote Code Execution Vulnerability** ***Bhdresh (Aug 07)***
  - Re: [FD] ManageEngine ADSelfService Plus – Unauthenticated Remote Code Execution Vulnerability *Bhdresh (Aug 11)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License