

شنو هاد
FIRESTARTER؟

ALERT: HIGH PRIORITY
CISA • Cisco • FIRESTARTER
SYSTEM COMPROMISED.
PERSISTENT BACKDOOR DETECTED.

060T
0810 615E0
00FS0P0ES,
CEB18)
1001201
090
FIS1185
0882036
S 2.6H
CONPROG
PERSIST BACKDOOR
GB014

المشکل کبیر

Corrupted web traffic logs
Corrupted web trafts orc: %3916\$ \$syric\$ _arnts
Comressed staim:raas [fer="uts"]
Etatihic traffic logs
Corrupted web data srr:LTEVJEA
Suppressed syslog line
Suppressed syslog line
Suppressed syslog line
Suppressed digital line st=381
Corrupted logs change= %9317S \$syric\$ _arnts

UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849

Corrupted web traffic logs t oces oia tao weleft
outpfoeed evelog tinerion Scappf6ctigerp _arnts
Ganncead perdnital abonoseshos.
Corrupted web comraoedifg
Corrupted web co tochee
Corrupted web traffic boe= %9317S \$syric\$ _arnts
Suppreceed oiairtraffios loga
Gannad eodie loga
Suppreed web kmto ooe= *22R/6G1HCO168
Suppreceadly auto caes 169
Con laofed borror arirrepte oer: %98177S Seyric\$ _arnts
Snieo traffic lootr ann eetes tia to "L89"
Supprecead weevia not tavies ceocesdorga.
Sihnressed eiof pathue: Umtoasios1
Snhprecead digital line
Gornneced aigon Inno atn=385
Comrupted loge changee= %90017S Seyric\$ _arnts

UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849
UAT4356 Storm-1849



نقرا الـ logs دابا



BOOT SCRIPTS ANALYSIS

```
sc
nc
ascm
mov    add, rex, --
mov    asd, rex
mov    assem [root..Bo00]
call   ard, 0x4001a1
mov    rex
mov    seda
mov    edx
mov    asd, end
call
```

>>> [ALERT]: Potential LINA hooking indicator detected at address 0x4010a3 <<<

```
> _lina_hook_init
_lina_hook_init ->
system call interposer_inits
sstem call std_$nita

=> system call interposer

if (it -l then:
system call interposer -> $in
fi
```

PACKET CAPTURES / CVE DB

```
PACKET CAPTURES / CVE DB
Packet packets
Packet packets
Packet D: 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 0a 01 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
```

REFERENCE: CVE-2025-20333
[Buffer Overflow in LINA module]

REFERENCE: CVE-2025-20362
[Unauthenticated RCE in boot process]

LOG FILES & MOUNT LIST

```
$ ls -lR
.
├── boot
├── src
│   ├── ...
│   ├── lina
│   │   ├── /dev/mapper/root_hook
│   │   ├── /dev/mapper/root
│   │   ├── /dev/mapper/root_hook
│   │   ├── /opt/beot/custom_lina_init.sh
│   │   ├── /opt/beot/custom_lina_init.sh
│   │   └── /opt/boot/custom_lina_init.sh
│   ├── ...
├── mounts
└── moun_s
```


خسرتو

نطبق ال Patch دابا

CISA • NCSC • CISCO
ADVISORY

```
EXEC_RESTART_COMPLETE: OK  
REINAGE_WORKFLDN: ACTIVE  
APPLYING_PATCHES_3/5
```

