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


المشكل كبير
Corrupted webtraffic logs
Corrupted web traffics orc: %3916$ $syric$ _.anttts
Suppressed digital line st=381
Corrupted logs change= %93175 $syric$ _.anttts
UAT4356 Storm-1849
LINE VIPER TOOLS
Cisco
Firepower

BOOT SCRIPTS ANALYSIS

```
mov     asd, rex
mov     assm [root_boot]
call    ard, 0x4001a1
mov     rex
mov     seda
mov     edx
call    asd, end

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

> _lina_hook_init
_lina_hook_init ->
system call interpser_inits
system call std_inita

> 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 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/boot/custom_lina_init.sh
│   │   ├── /opt/beot/custom_lina_init.sh
│   │   └── /opt/boot/custom_lina_init.sh
│   ├── ...
│   └── mounts
└── moun_s
```


خسرتو
نطبّق الPatch دابا
CISA • NCSC • CISCO
ADVISORY
EXEC_RESTART_COMPLETE: OK
REINAGE_WORKFLDN: ACTIVE
APPLYING_PATCHES_3/5
CISCO
Firepower