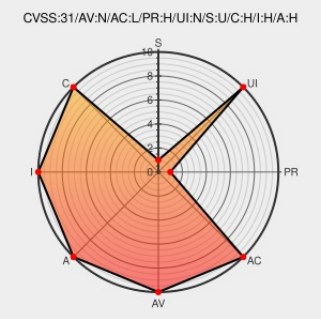
CVE-2020-16148

Published on: 09/24/2020 12:00:00 AM UTC

Last Modified on: 04/28/2022 06:21:00 PM UTC

CVE-2020-16148

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Accesslog from Telmat contain the following vulnerability:

The ping page of the administration panel in Telmat AccessLog <= 6.0 (TAL_20180415) allows an attacker to get root shell access via authenticated code injection over the network.

CVE-2020-16148 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
CVE-2020-16148 - Telmat - Authenticated root RCE · Podalirius	Exploit, Third Party Advisory, podalirius.net, text/html	MISC podalirius.net/cves/2020-16148/

CVE-2020-16148 - Telmat - Authenticated root RCE · Podalirius podalirius.net text/html MISC podalirius.net/en/cves/2020-16148/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Telmat	Accesslog	-	All	All	All
Hardware	Telmat	Accesslog	-	All	All	All
Operating System	Telmat	Accesslog Firmware	All	All	All	All
Operating System	Telmat	Accesslog Firmware	All	All	All	All
Hardware	Telmat	Educ@box	-	All	All	All
Hardware	Telmat	Educ@box	-	All	All	All
Operating System	Telmat	Educ@box Firmware	All	All	All	All
Operating System	Telmat	Educ@box Firmware	All	All	All	All
Hardware	Telmat	Git@box	-	All	All	All
Hardware	Telmat	Git@box	-	All	All	All
Operating System	Telmat	Git@box Firmware	All	All	All	All
Operating System	Telmat	Git@box Firmware	All	All	All	All

cpe:2.3:h:telmat:accesslog:-:*:*:*:*:*:*:*:

cpe:2.3:h:telmat:accesslog:-:*:*:*:*:*:*:*:

cpe:2.3:o:telmat:accesslog_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:telmat:accesslog_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:telmat:educ\@box:-:*:*:*:*:*:*:*:

cpe:2.3:h:telmat:educ\@box:-:*:*:*:*:*:*:*:

cpe:2.3:o:telmat:educ\@box_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:telmat:educ\@box_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:telmat:git\@box:-:*:*:*:*:*:*:*:

cpe:2.3:h:telmat:git\@box:-:*:*:*:*:*:*:*:

cpe:2.3:o:telmat:git\@box_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:telmat:git\@box_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Git - CVE-2020-16148: podalirius.net/cves/2020-1614…	2021-06-14 12:55:22
@RemotelyAlerts	Severity: ??? | The ping page of the administration pane... | CVE-2020-16148 | Link for more: alerts.remotelyrmm.com/CVE-2020-16148	2022-04-28 19:35:21

← Previous ID

Next ID→