

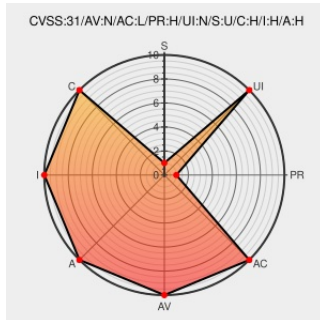


CVE-2019-10669

Published on: 09/09/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:39 PM UTC

CVE-2019-10669

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Librenms](#) from [Librenms](#) contain the following vulnerability:

An issue was discovered in LibreNMS through 1.47. There is a command injection vulnerability in `html/includes/graphs/device/collectd.inc.php` where user supplied parameters are filtered with the `mysqli_escape_real_string` function.

This function is not the appropriate function to sanitize command arguments as it does not escape a number of command line syntax characters such as ` (backtick), allowing an attacker to inject commands into the variable `$rrd_cmd`, which gets executed via `passthru()`.

CVE-2019-10669 has been assigned by [M](#) 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: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

404 Not Found

Exploit

Third Party Advisory

www.darkmatter.ae

text/html

Inactive Link

Not Archived

MISC

www.darkmatter.ae/xen1thlabs/librenms-command-injection-vulnerability-xl-19-017/

LibreNMS Collectd Command Injection ≈ Packet Storm

Exploit

Third Party Advisory

VDB Entry

packetstormsecurity.com

text/html

MISC

packetstormsecurity.com/files/154391/LibreNMS-Collectd-Command-Injection.html

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
Application	Librenms	Librenms	All	All	All	All

cpe:2.3:a:librenms:librenms:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →