



CVE-2019-12463

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

Last Modified on: 03/23/2021 11:27:41 PM UTC

CVE-2019-12463

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

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

An issue was discovered in LibreNMS 1.50.1. The scripts that handle graphing options (includes/html/graphs/common.inc.php and includes/html/graphs/graphs.inc.php) do not sufficiently validate or encode several fields of user supplied input. Some parameters are filtered with `mysqli_real_escape_string`, which is only useful for

preventing SQL injection attacks; other parameters are unfiltered. This allows an attacker to inject RRDtool syntax with newline characters via the `html/graph.php` and `html/graph-realtime.php` scripts. RRDtool syntax is quite versatile and an attacker could leverage this to perform a number of attacks, including disclosing directory structure and filenames, disclosing file content, denial of service, or writing arbitrary files. NOTE: relative to CVE-2019-10665, this requires authentication and the pathnames differ.

CVE-2019-12463 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	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-rrdtool-injection-vulnerability-xl-19-022/

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
Application	Librenms	Librenms	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→