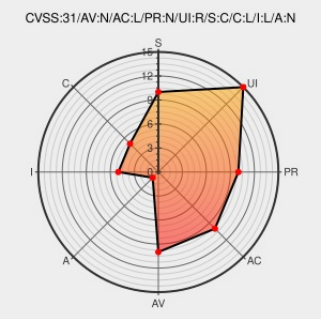
CVE-2019-10670

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

Last Modified on: 03/23/2021 11:27:40 PM UTC

CVE-2019-10670

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. Many of the scripts rely on the function mysqli_escape_real_string for filtering data. However, this is particularly ineffective when returning user supplied input in an HTML or a JavaScript context, resulting in unsafe data being injected into these contexts, leading to attacker controlled JavaScript executing in the browser. One example of this is the string parameter in html/pages/inventory.inc.php.

CVE-2019-10670 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
404 Not	Exploit	MISC www.darkmatter.ae/xen1thlabs/librenms-multiple-reflected-cross-site-scripting

404 Not Found	Exploit Third Party Advisory www.darkmatter.ae text/html Inactive Link Not Archived	MISC www.darkmatter.ae/xen1thlabs/librenms-multiple-reflected-cross-site-scripting-vulnerability-xl-19-021/

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→