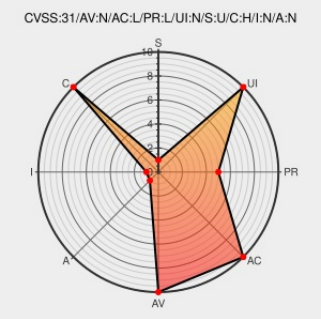
CVE-2020-15873

Published on: 07/21/2020 12:00:00 AM UTC

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

CVE-2020-15873

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



Certain versions of Librenms from Librenms contain the following vulnerability:

In LibreNMS before 1.65.1, an authenticated attacker can achieve SQL Injection via the customoid.inc.php device_id POST parameter to ajax_form.php.

CVE-2020-15873 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Fix sql injection (#11923) · librenms/librenms@8f3a29c · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/librenms/librenms/commit/8f3a29cde5bbd8608f9b42923a7d7e2598bcac4

Comparing 1.65...1.65.1 · librenms/librenms · GitHub	Third Party Advisory github.com text/html	MISC github.com/librenms/librenms/compare/1.65...1.65.1
Fix sql injection by murrant · Pull Request #11923 · librenms/librenms · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/librenms/librenms/pull/11923
CVE-2020-15873: Blind SQL Injection in Librenms - Loginsoft Research	Exploit Third Party Advisory research.loginsoft.com text/html	MISC research.loginsoft.com/bugs/blind-sql-injection-in-librenms/
Announcements - LibreNMS Community	Release Notes Vendor Advisory community.librenms.org text/html	MISC community.librenms.org/c/announcements

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

Exploit/POC from Github

Proof of Concept of CVE-2020-15873 - Blind SQL Injection in Librenms < v1.65.1

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→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report