huntr

Improper Authorization in librenms/librenms

✔ Valid   Reported on Feb 12th 2022

Description

LibreNMS v22.1.0 allows users with the normal role/level to interact with the plugin setting resulting in the users could take action such as switching on/off any installed plugins which are supposedly accessible by the Administrator only.

Proof of Concept

Affected endpoints:

1 GET http://{HOST}/plugin/settings

~

Steps to reproduce:

1 Login as a normal user.

2 Browse to http://{HOST}/plugin/settings

3 We can switch on/off any installed plugins and interact with the setting such as creating and managing maps for the Weathermap plugin.

Impact

This vulnerability is capable of modifying or performing a system function outside the user's limits.

CVE
CVE-2022-0587
(Published)

Vulnerability Type
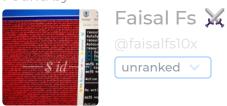CWE-285: Improper Authorization

Severity
High (7.1)

Visibility
Public

Chat with us

Status
Fixed

Found by

Faisal Fs ⚔️
@faisalfs10x

unranked ⌄

We are processing your report and will contact the **librenms** team within 24 hours. 9 months ago

Faisal Fs ⚔️ modified the report 9 months ago

We have contacted a member of the **librenms** team and are waiting to hear back 9 months ago

PipoCanaja validated this vulnerability 9 months ago

Faisal Fs ⚔️ has been awarded the disclosure bounty ✔️

The fix bounty is now up for grabs

Neil Lathwood marked this as fixed in **22.2.0** with commit **95970a** 9 months ago

The fix bounty has been dropped ❌

This vulnerability will not receive a CVE ❌

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us