Improper Access Control in librenms/librenms

1

Valid Reported on Feb 12th 2022

Description

Improper Access Control vulnerability in LibreNMS v22.1.0 allows attackers with the normal role/level to interact with port-groups functionality such as create, edit/modify and delete the existing port group. The port-groups functionality fails to enforce policy such that normal users could act outside of their intended permissions which are supposedly accessible by the Administrator only.

Proof of Concept

Affected endpoints:
1 GET http://{HOST}/port-groups - [view all port groups]
2 POST http://{HOST}/port-groups - [create]
3 POST http://{HOST}/port-groups/{port_id} - [edit]
4 DELETE http://{HOST}/port-groups/{port_id} - [delete]
~
Steps to reproduce:
1 Login as normal user.
2 Browse to http://{HOST}/port-groups.
3 We can interact with the port group functionality such as create, edit/modify and delete existing port group.

Impact

This vulnerability is capable of leading to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

Occurrences

form.blade.php L4-L12

CVE
CVE-2022-0580
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
High (7.1)

Visibility
Public

Status
Fixed

Found by

Faisal Fs ⚔️
@faisalfs10x
unranked

This report was seen 382 times.

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

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 ✖

form.blade.php#L4-L12 has been validated

Sign in to join this conversation