Cross-site Scripting (XSS) - Stored in librenms/librenms

0

Valid Reported on Feb 12th 2022

Description

Stored XSS in create/modify Transport Groups, Add/Edit Service and Edit Service Template

Proof of Concept

Payload:

```
'><body onload=alert(/XSS/)>
```

~

PoC image:

Xss payload in create/modify Transport Groups

Xss payload in Add/Edit Service

Xss payload in Edit Service Template

~

XSS will fire-up by user visiting:

1 http://{HOST}/alert-transports

2 http://{HOST}/device/{id}/services

Impact

This vulnerability is capable of running malicious javascript code on web pages.

CVE

CVE-2022-0589

(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Stored

Severity

Medium (5.4)

Visibility

Public

Status
Fixed

Found by

Faisal Fs ⚔️
@faisalfs10x
unranked

Fixed by

PipoCanaja
@pipocanaja
maintainer

This report was seen 409 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

Faisal Fs ⚔️ modified the report 9 months ago

Faisal Fs ⚔️ modified the report 9 months ago

Faisal Fs ⚔️ modified the report 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

PipoCanaja marked this as fixed in **22.1.0** with commit **4c9d4e** 9 months ago

PipoCanaja has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation