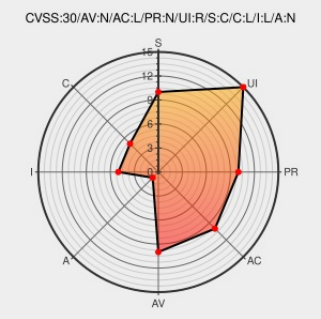
# CVE-2019-1000024

Published on: 02/04/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:02:00 AM UTC

## CVE-2019-1000024

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




Certain versions of Ng-netms from Opt-net contain the following vulnerability:

OPT/NET BV NG-NetMS version v3.6-2 and earlier versions contains a Cross Site Scripting (XSS) vulnerability in /js/libs/jstree/demo/filebrowser/index.php page. The "id" and "operation" GET parameters can be used to inject arbitrary JavaScript which is returned in the page's response that can result in Cross-site scripting.This attack appear to be exploitable via network connectivity.

CVE-2019-1000024 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 6.1 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| CHANGED | LOW | LOW | NONE |

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| OPTOSS NG-NetMS \| SourceForge.net | Product<br>Third Party Advisory | MISC sourceforge.net/projects/ngnms/ |

| | | |
|---|---|---|
| | sourceforge.net<br>text/html | |
| Cross-site scripting (XSS) in OPTOSS Next Gen Network Management System (NG-NetMS) - Information security | web.archive.org<br>text/html<br>Inactive Link Not Archived | MISC inf0seq.github.io/cve/2019/01/20/Cross-site-scripting-(XSS)-in-OPTOSS-Next-Gen-Network-Management-System-(NG-NetMS).html |
| Cross-site Scripting (XSS) - OWASP | Third Party Advisory<br>www.owasp.org<br>text/html | MISC www.owasp.org/index.php/Cross-site_Scripting_(XSS) |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Opt-net | Ng-netms | All | All | All | All |

cpe:2.3:a:opt-net:ng-netms:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→