

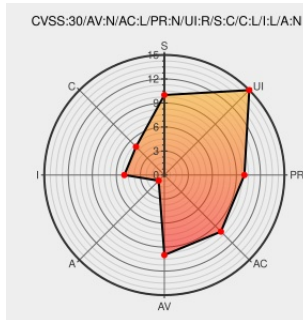


CVE-2017-16224

Published on: 06/06/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:38 PM UTC

CVE-2017-16224

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [St](#) from [St Project](#) contain the following vulnerability:

st is a module for serving static files. An attacker is able to craft a request that results in an HTTP 301 (redirect) to an entirely different domain. A request for:

`http://some.server.com//nodesecurity.org/%2e%2e` would result in a 301 to `//nodesecurity.org/%2e%2e` which most browsers treat as a

proper redirect as `//` is translated into the current schema being used. Mitigating factor: In order for this to work, st must be serving from the root of a server (`/`) rather than the typical sub directory (`/static/`) and the redirect URL will end with some form of URL encoded `..` ("`%2e%2e`", "`%2e.`", "`%.%2e`").

CVE-2017-16224 has been assigned by [h1](#) support@hackerone.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [h1](#) **HackerOne** - **st node module** version `<=1.2.1`

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: **5.8 - MEDIUM**

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

CVE References

Description

Tags

Link

Overview

Exploit

Third Party Advisory

nodesecurity.io

text/html

S MISC nodesecurity.io/advisories/547

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type

Vendor

Product

Version

Update

Edition

Language

Application

[St Project](#)

[St](#)

All

All

All

All

cpe:2.3:a:st_project:st:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)