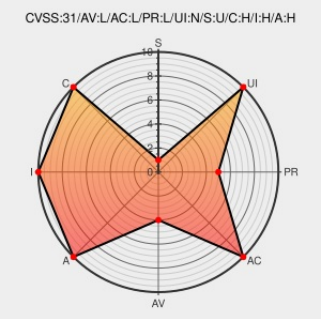
CVE-2020-7615

Published on: 04/07/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:53 PM UTC

CVE-2020-7615

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



Certain versions of Fsa from Fsa Project contain the following vulnerability:

fsa through 0.5.1 is vulnerable to Command Injection. The first argument of 'execGitCommand()', located within 'lib/rep.js#63' can be controlled by users without any sanitization to inject arbitrary commands.

CVE-2020-7615 has been assigned by report@snyk.io to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Command Injection in fsa | Snyk	Exploit, Third Party Advisory, snyk.io, text/html	MISC snyk.io/vuln/SNYK-JS-FSA-564118

fsa/rep.js at master · gregof/fsa · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/gregof/fsa/blob/master/lib/rep.js#L12

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fsa Project	Fsa	All	All	All	All

cpe:2.3:a:fsa_project:fsa:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→