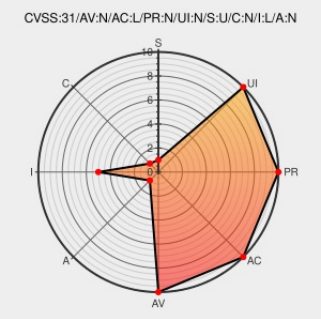
CVE-2020-7638

Published on: 04/06/2020 12:00:00 AM UTC

Last Modified on: 12/02/2022 07:58:00 PM UTC

CVE-2020-7638

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



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

confinit through 0.3.0 is vulnerable to Prototype Pollution.The 'setDeepProperty' function could be tricked into adding or modifying properties of 'Object.prototype' using a '__proto__' payload.

CVE-2020-7638 has been assigned by report@snyk.io to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Prototype Pollution in confinit | Snyk	Exploit, Third Party Advisory, snyk.io, text/html	MISC snyk.io/vuln/SNYK-JS-CONFINIT-564433

Close #1 · davideicardi/confinit@a34e06c · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/davideicardi/confinit/commit/a34e06ca5c1c8b047ef112ef188b2fe30d2a1ea

Related QID Numbers

981897 Nodejs (npm) Security Update for confinit (GHSA-jgpq-g82g-6c39)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:confinit_project:confinit:*:*:*:*:*:node.js:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→