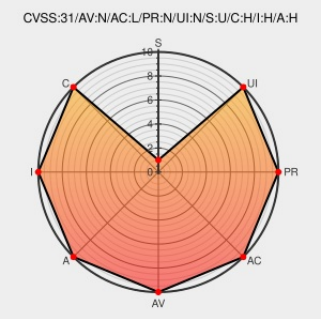
CVE-2020-28273

Published on: 12/02/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:27 PM UTC

CVE-2020-28273

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



Certain versions of Set-in from Set-in Project contain the following vulnerability:

Prototype pollution vulnerability in 'set-in' versions 1.0.0 through 2.0.0 allows attacker to cause a denial of service and may lead to remote code execution.

CVE-2020-28273 has been assigned by vulnerabilitylab@whitesourcesoftware.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
fix prototype pollution vulnerability · ahdinosaur/set-in@e431eff · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ahdinosaur/set-in/commit/e431effa00195a6f06b111e09733cd1445a91a88

Open Source Vulnerabilities Database - WhiteSource	Third Party Advisory www.whitesourcesoftware.com text/html	MISC www.whitesourcesoftware.com/vulnerability-database
CVE-2020-28273 | WhiteSource Vulnerability Database	Exploit Third Party Advisory www.whitesourcesoftware.com text/html	MISC www.whitesourcesoftware.com/vulnerability-database/CVE-2020-28273

Related QID Numbers

982903 Nodejs (npm) Security Update for set-in (GHSA-qr4p-c9wr-phr6)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Set-in Project	Set-in	All	All	All	All

cpe:2.3:a:set-in_project:set-in:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→