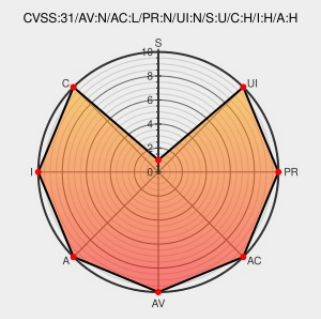
CVE-2020-12265

Published on: 04/26/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-12265

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



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

The decompress package before 4.2.1 for Node.js is vulnerable to Arbitrary File Write via ../ in an archive member, when a symlink is used, because of Directory Traversal.

CVE-2020-12265 has been assigned by cve@mitre.org 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
Overview	Third Party Advisory www.npmjs.com text/html	MISC www.npmjs.com/advisories/1217
Prevent directory traversal by trptcolin · Pull Request #73 ·	Patch	MISC

kevva/decompress · GitHub	Third Party Advisory github.com text/html	github.com/kevva/decompress/pull/73
Vulnerable to zip slip · Issue #71 · kevva/decompress · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/kevva/decompress/issues/71

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.

Related QID Numbers

981891 Nodejs (npm) Security Update for decompress (GHSA-qgfr-5hqp-vrw9)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:decompress_project:decompress:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:decompress_project:decompress:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→