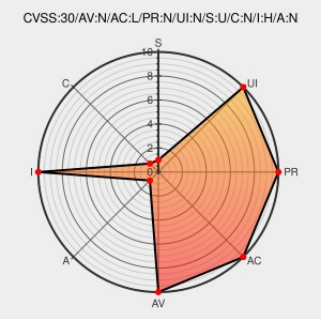
CVE-2018-20834

Published on: 04/30/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:36 PM UTC

CVE-2018-20834

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



Certain versions of Node-tar from Node-tar Project contain the following vulnerability:

A vulnerability was found in node-tar before version 4.4.2 (excluding version 2.2.2). An Arbitrary File Overwrite issue exists when extracting a tarball containing a hardlink to a file that already exists on the system, in conjunction with a later plain file with the same name as the hardlink. This plain file content replaces the existing file content. A patch has been applied to node-tar v2.2.2).

CVE-2018-20834 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
Comparing 58a8d43...a5f7779 · npm/node-tar · GitHub	Patch Third Party Advisory	MISC github.com/npm/node-tar/compare/58a8d43...a5f7779

	github.com text/html	
Bump fstream to fix hardlink overwriting vulnerability · npm/node-tar@7ecef07 · GitHub	github.com text/html	MISC github.com/npm/node-tar/commit/7ecef07da6a9e72cc0c4d0c9c6a8e85b6b52395d
Commits · npm/node-tar · GitHub	github.com text/html	MISC github.com/npm/node-tar/commits/v2.2.2
NVD - CVE-2018-20834	nvd.nist.gov text/html	MISC nvd.nist.gov/vuln/detail/CVE-2018-20834
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:1821
HackerOne	Exploit Third Party Advisory hackerone.com text/html	MISC hackerone.com/reports/344595
unpack: only reuse file fs entries if nlink = 1 · npm/node-tar@b0c5843 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/npm/node-tar/commit/b0c58433c22f5e7fe8b1c76373f27e3f81dcd4c8

Related QID Numbers

981797 Nodejs (npm) Security Update for tar (GHSA-j44m-qm6p-hp7m)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Node-tar Project	Node-tar	All	All	All	All
Application	Node-tar Project	Node-tar	All	All	All	All

cpe:2.3:a:node-tar_project:node-tar:*:*:*:*:*:*:*:*:

cpe:2.3:a:node-tar_project:node-tar:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report