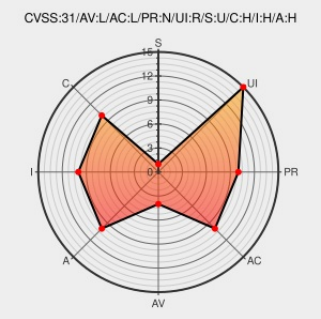
CVE-2019-10773

Published on: 12/16/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:39 PM UTC

CVE-2019-10773

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



Certain versions of Yarn from Yarnpkg contain the following vulnerability:

In Yarn before 1.21.1, the package install functionality can be abused to generate arbitrary symlinks on the host filesystem by using specially crafted "bin" keys. Existing files could be overwritten depending on the current user permission set.

CVE-2019-10773 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	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
[SECURITY] Fedora 30 Update: nodejs-yarn-1.21.1-1.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org, text/html	FEDORA FEDORA-2020-7525beefa1

Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2020:0475
Fixes bin overwrites (#7755) · yarnpkg/yarn@039bafd · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/yarnpkg/yarn/commit/039bafd74b7b1a88a53a54f8fa6fa872615e90e7
[SECURITY] Fedora 31 Update: nodejs-yarn-1.21.1-1.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-766ce5adae
Invalid vulnerability	Broken Link snyk.io text/html Inactive Link Not Archived	MISC snyk.io/vuln/SNYK-JS-YARN-537806,
globally-installed package overwrites an existing binary in the target install location · Issue #7761 · yarnpkg/yarn · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/yarnpkg/yarn/issues/7761#issuecomment-565493023
binary planting and arbitrary file (over)write vulnerabilities in npm, pnpm and yarn | Blog of Daniel Ruf	Exploit Third Party Advisory blog.daniel-ruf.de text/html	DR MISC blog.daniel-ruf.de/critical-design-flaw-npm-pnpm-yarn/

Related QID Numbers

981590 Nodejs (npm) Security Update for yarn (GHSA-5xf4-f2fq-f69j)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yarnpkg	Yarn	All	All	All	All
Application	Yarnpkg	Yarn	All	All	All	All

cpe:2.3:a:yarnpkg:yarn:*:*:*:*:*:*:*:*:

cpe:2.3:a:yarnpkg:yarn:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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