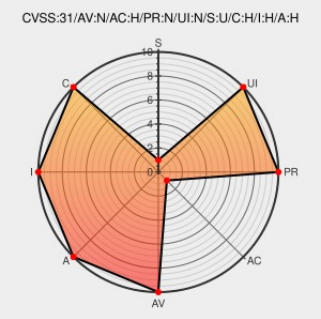
CVE-2019-5448

Published on: 07/30/2019 12:00:00 AM UTC

Last Modified on: 11/03/2021 06:27:00 PM UTC

CVE-2019-5448

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



Certain versions of Yarn from Yarnpkg contain the following vulnerability:

Yarn before 1.17.3 is vulnerable to Missing Encryption of Sensitive Data due to HTTP URLs in lockfile causing unencrypted authentication data to be sent over the network.

CVE-2019-5448 has been assigned by support@hackerone.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **yarn** - **yarn** version **Fixed in 1.17.3**

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
HackerOne	Permissions Required Third Party Advisory hackerone.com	MISC hackerone.com/reports/640904

	text/html	
notes/Yarn-vuln.md at master · ChALkeR/notes · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/ChALkeR/notes/blob/master/Yarn-vuln.md
Recommended security update | Yarn Blog	Vendor Advisory yarnpkg.com text/html	CONFIRM yarnpkg.com/blog/2019/07/12/recommended-security-update/

Related QID Numbers

980214 Nodejs (npm) Security Update for yarn (GHSA-wqfc-cr59-h64p)

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

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→