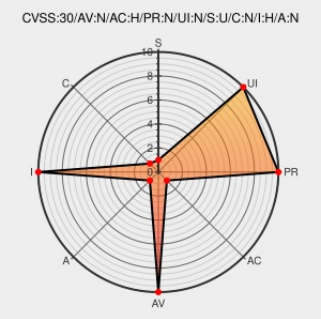
CVE-2018-12556

Published on: 05/16/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:22 PM UTC

CVE-2018-12556

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



Certain versions of Website from Yarnpkg contain the following vulnerability:

The signature verification routine in install.sh in yarnpkg/website through 2018-06-05 only verifies that the yarn release is signed by any (arbitrary) key in the local keyring of the user, and does not pin the signature to the yarn release key, which allows remote attackers to sign tampered yarn release packages with their own key.

CVE-2018-12556 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Johnny-You-Are-Fired/johnny-fired.pdf at master · RUB-NDS/Johnny-You-Are-Fired · GitHub	Third Party Advisory github.com text/html	MISC github.com/RUB-NDS/Johnny-You-Are-Fired/blob/master/paper/johnny-fired.pdf

GitHub - RUB-NDS/Johnny-You-Are-Fired: Artifacts for the USENIX publication.	Third Party Advisory github.com text/html	MISC github.com/RUB-NDS/Johnny-You-Are-Fired
Johnny You Are Fired ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/152703/Johnny-You-Are-Fired.html
Commits · yarnpkg/website · GitHub	Third Party Advisory github.com text/html	MISC github.com/yarnpkg/website/commits/master
Full Disclosure: OpenPGP and S/MIME signature forgery attacks in multiple email clients	Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20190430 OpenPGP and S/MIME signature forgery attacks in multiple email clients
oss-security - Spoofing OpenPGP and S/MIME Signatures in Emails (multiple clients)	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20190430 Spoofing OpenPGP and S/MIME Signatures in Emails (multiple clients)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:yarnpkg:website:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→