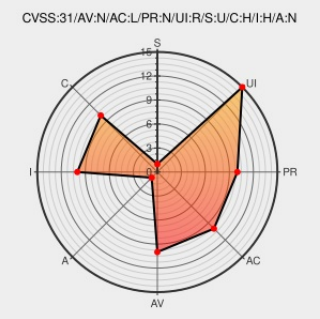
CVE-2020-26226

Published on: 11/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:55 PM UTC

CVE-2020-26226 - advisory for GHSA-r2j6-p67h-q639

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



Certain versions of Semantic-release from Semantic-release Project contain the following vulnerability:

In the npm package semantic-release before version 17.2.3, secrets that would normally be masked by `semantic-release` can be accidentally disclosed if they contain characters that become encoded when included in a URL. Secrets that do not contain characters that become encoded when included in a URL are already masked properly. The issue is fixed in version 17.2.3.

CVE-2020-26226 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **semantic-release** - **semantic-release** version **< 6.1.5**

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link

Secret disclosure when containing characters that become URI encoded · Advisory · semantic-release/semantic-release · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/semantic-release/semantic-release/security/advisories/GHSA-r2j6-p67h-q639
fix: mask secrets when characters get uri encoded · semantic-release/semantic-release@ca90b34 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/semantic-release/semantic-release/commit/ca90b34c4a9333438cc4d69faeb43362bb991e5a

Related QID Numbers

983219 Nodejs (npm) Security Update for semantic-release (GHSA-r2j6-p67h-q639)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Semantic-release Project	Semantic-release	All	All	All	All
Application	Semantic-release Project	Semantic-release	All	All	All	All

cpe:2.3:a:semantic-release_project:semantic-release:*:*:*:*:*:*:*:*:

cpe:2.3:a:semantic-release_project:semantic-release:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→