

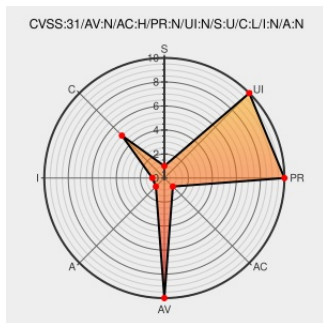


CVE-2020-15262

Published on: 10/19/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 04:19:00 PM UTC

CVE-2020-15262 - advisory for GHSA-4fc4-chg7-h8gh

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Webpack-subresource-integrity](#) from [Webpack-subresource-integrity Project](#) contain the following vulnerability:

In webpack-subresource-integrity before version 1.5.1, all dynamically loaded chunks receive an invalid integrity hash that is ignored by the browser, and therefore the browser cannot validate their integrity. This removes the additional level of protection offered by SRI for such chunks. Top-level chunks are unaffected. This issue is patched in

version 1.5.1.

CVE-2020-15262 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **LOW** severity.

Affected Vendor/Software: waysact - webpack-subresource-integrity version < 1.5.1

CVSS3 Score: **3.7 - LOW**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

Fix hash lookup for dynamic chunks · waysact/webpack-subresource-integrity@3d7090c · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC github.com/waysact/webpack-subresource-integrity/commit/3d7090c08c333fcb10ad9e2d6cf72e2acb7d87f

Tags are injected with integrity="undefined" on v1.5.0 · Issue #131 · waysact/webpack-subresource-integrity · GitHub

Third Party Advisory

github.com

text/html

MISC github.com/waysact/webpack-subresource-integrity/issues/131

Unprotected dynamically loaded chunks · Advisory · waysact/webpack-subresource-integrity · GitHub

Third Party Advisory

github.com

text/html

CONFIRM github.com/waysact/webpack-subresource-integrity/security/advisories/GHSA-4fc4-chg7-h8gh

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

980064 Nodejs (npm) Security Update for webpack-subresource-integrity (GHSA-4fc4-chg7-h8gh)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Webpack-subresource-integrity Project	Webpack-subresource-integrity	All	All	All	All
Application	Webpack-subresource-integrity Project	Webpack-subresource-integrity	All	All	All	All

cpe:2.3:a:webpack-subresource-integrity_project:webpack-subresource-integrity:*:*:*:*:node.js:*:*:

cpe:2.3:a:webpack-subresource-integrity_project:webpack-subresource-integrity:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID →

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)