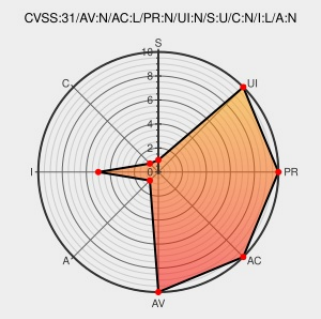
CVE-2022-35948

Published on: Not Yet Published

Last Modified on: 03/28/2023 05:08:00 PM UTC

CVE-2022-35948 - advisory for GHSA-f772-66g8-q5h3

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



Certain versions of Undici from Nodejs contain the following vulnerability:

undici is an HTTP/1.1 client, written from scratch for Node.js.`=< undici@5.8.0` users are vulnerable to _CRLF Injection_ on headers when using unsanitized input as request headers, more specifically, inside the `content-type` header. Example: ``` import { request } from 'undici' const unsanitizedContentTypeInput = 'application/json\r\n\r\nGET /foo2 HTTP/1.1' await request('http://localhost:3000, { method: 'GET', headers: { 'content-type': unsanitizedContentTypeInput }, }) ``` The above snippet will perform two requests in a single `request` API call: 1) `http://localhost:3000/` 2) `http://localhost:3000/foo2` This issue was patched in Undici v5.8.1. Sanitize input when sending content-type headers using user input as a workaround.

CVE-2022-35948 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **nodejs** - **undici** version **=< 5.8.0**

CVSS3 Score: 5.3 - MEDIUM

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

CVE References

Description	Tags	Link
Merge pull request from GHSA-f772-66g8-q5h3 · nodejs/undici@66165d6 · GitHub	github.com text/html	MISC github.com/nodejs/undici/commit/66165d604fd0aee70a93ed5c44ad4cc2df395f80

Release v5.8.2 · nodejs/undici · GitHub	github.com text/html	MISC github.com/nodejs/undici/releases/tag/v5.8.2
CRLF Injection in Nodejs 'undici' via Content-Type · Advisory · nodejs/undici · GitHub	github.com text/html	CONFIRM github.com/nodejs/undici/security/advisories/GHSA-f772-66g8-q5h3

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

184306 Debian Security Update for node-undici (CVE-2022-35948)

753302 SUSE Enterprise Linux Security Update for nodejs16 (SUSE-SU-2022:3251-1)

753318 SUSE Enterprise Linux Security Update for nodejs16 (SUSE-SU-2022:3250-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nodejs	Undici	All	All	All	All

cpe:2.3:a:nodejs:undici:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@matteocollina	CVE-2022-35948 is about a CRLF Injection in Nodejs 'undici' via Content-Type. github.com/nodejs/undici/…	2022-08-09 09:45:29
@CVEreport	CVE-2022-35948 : undici is an HTTP/1.1 client, written from scratch for Node.js.`=< undici@5.8.0` users are vulnera… twitter.com/i/web/status/1…	2022-08-13 23:36:03
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-35948 undici is an HTTP/1.1 client, written from scratch for Node.js.`=… twitter.com/i/web/status/1…	2022-08-14 01:56:00
@Har_sia	CVE-2022-35948 har-sia.info/CVE-2022-35948… #HarsiaInfo	2022-08-15 07:01:05
@LinInfoSec	Nodejs - CVE-2022-35948: github.com/nodejs/undici/…	2022-08-15 13:18:14
/r/netcve	CVE-2022-35948	2022-08-14 00:38:40

← 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 registred 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