



CVE-2022-31070

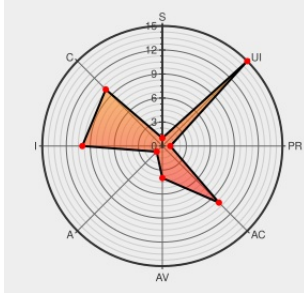
Published on: Not Yet Published

Last Modified on: 07/05/2022 07:58:00 PM UTC

CVE-2022-31070 - advisory for GHSA-77mv-4rg7-r8qv

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

CVSS:31/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N



Certain versions of [Nestjs-proxy](#) from [Finastra](#) contain the following vulnerability:

NestJS Proxy is a NestJS module to decorate and proxy calls. Prior to version 0.7.0, the nestjs-proxy library did not have a way to block sensitive cookies (e.g. session cookies) from being forwarded to backend services configured by the application developer. This could have led to sensitive cookies being inadvertently exposed to such

services that should not see them. The patched version now blocks cookies from being forwarded by default. However developers can configure an allow-list of cookie names by using the `allowedCookies` config setting. This issue has been fixed in version 0.7.0 of `@finastra/nestjs-proxy`. Users of `@ffdc/nestjs-proxy` are advised that this package has been deprecated and is no longer being maintained or receiving updates. Such users should update their package.json file to use `@finastra/nestjs-proxy` instead.

CVE-2022-31070 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Finastra](#) - [finastra-nodejs-libs](#) version < 0.7.0

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

PARTIAL

NONE

NONE

CVE References

Description	Tags	Link
[Proxy] cookies forwarding by bclvdv · Pull Request #232 · Finastra/finastra-nodejs-lib · GitHub	github.com text/html	MISC github.com/Finastra/finastra-nodejs-lib/pull/232
Potential Sensitive Cookie Exposure in NPM Packages @finastra/nestjs-proxy, @ffdc/nestjs-proxy · Advisory · Finastra/finastra-nodejs-lib · GitHub	github.com text/html	CONFIRM github.com/Finastra/finastra-nodejs-lib/security/advisories/GHSA-77mv-4rg7-r8qv

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Finastra	Nestjs-proxy	All	All	All	All
Application	Nestjs-proxy Project	Nestjs-proxy	All	All	All	All

cpe:2.3:a:finastra:nestjs-proxy:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:nestjs-proxy_project:nestjs-proxy:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31070 : NestJS Proxy is a NestJS module to decorate and proxy calls. Prior to version 0.7.0, the nestjs-pr... twitter.com/i/web/status/1...	2022-06-15 19:20:42
@LinInfoSec	Nodejs - CVE-2022-31070: github.com/Finastra/finas...	2022-06-15 21:01:14
@botter_jp	NestJS Proxyに複数の脆弱性	2022-06-15 22:41:03
@RemotelyAlerts	Severity: ?? NestJS Proxy is a NestJS module to decor... CVE-2022-31070 Link for more: alerts.remotelyrmm.com/CVE-2022-31070	2022-07-05 21:28:32

← 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](#)