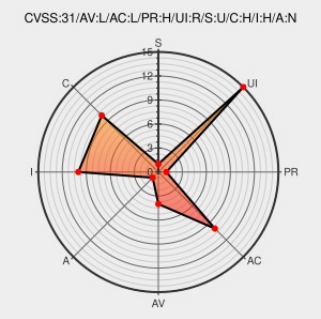
CVE-2022-31070

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



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 bcldvd · Pull Request #232 · Finastra/finastra-nodejs-libs · GitHub	github.com text/html	MISC github.com/Finastra/finastra-nodejs-libs/pull/232
Potential Sensitive Cookie Exposure in NPM Packages @finastra/nestjs-proxy, @ffdc/nestjs-proxy · Advisory · Finastra/finastra-nodejs-libs · GitHub	github.com text/html	CONFIRM github.com/Finastra/finastra-nodejs-libs/security/advisories/GHSA-77mv-4rg7-r8qv

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 and Source URL Uptime Status status.cve.report