



CVE-2022-35910

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-35910
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-19 13:15:00 UTC
Updated	2022-08-19 18:43:00 UTC
Description	In Jellyfin before 10.8, stored XSS allows theft of an admin access token.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jellyfin	Jellyfin	All	All	All	All

References

Reference	S
Require elevation to save list of plugin repositories by crobifero · Pull Request #7569 · jellyfin/jellyfin · GitHub	M
CVE-2022-35909 / CVE-2022-35910, Incorrect Access Control and XSS Stored to Jellyfin by Dan Barros stolabs Jul, 2022 Medium	M
Jellyfin - Google Docs	M
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report