



CVE-2023-38691

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-38691
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-04 17:15:00 UTC
Updated	2023-08-11 19:34:00 UTC
Description	matrix-appservice-bridge provides an API for setting up bridges. Starting in version 4.0.0 and prior to versions 8.1.2 and 9.0

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Matrix	Matrix-appservice-bridge	All	All	All	All
Application	Matrix	Matrix-appservice-bridge	9.0.0	All	All	All

References

Reference

[matrix-appservice-bridge doesn't verify the sub parameter of an openId token exchange, allowing unauthorized access to provisioning APIs · /](#)

[Merge pull request from GHSA-vc7j-h8xg-fv5x · matrix-org/matrix-appservice-bridge@4c6723a · GitHub](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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