



CVE-2021-32659

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

Summary

CVE	CVE-2021-32659
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-16 19:15:00 UTC
Updated	2021-07-09 19:46:00 UTC
Description	Matrix-appservice-bridge is the bridging service for the Matrix communication program's application services. In versions 2.6.0 and earlier, the service does not properly validate the 'room_id' parameter in the 'm.room.create' event, which can be used to bridge a room non-consensually.

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
Automatic room upgrade handling can be used maliciously to bridge a room non-consensually · Advisory · matrix-org/matrix-appservice-bridge
Check m.room.create event on room upgrade · matrix-org/matrix-appservice-bridge@b69e745 · GitHub
Release 2.6.1 (2021-06-02) · matrix-org/matrix-appservice-bridge · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[982090](#) Nodejs (npm) Security Update for matrix-appservice-bridge (GHSA-35g4-qx3c-vjhx)

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](#)