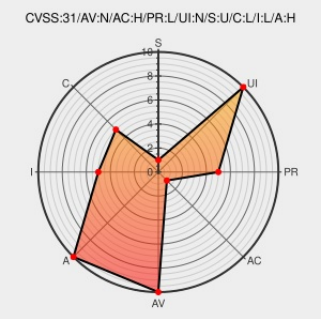
CVE-2022-31152

Published on: Not Yet Published

Last Modified on: 09/09/2022 03:21:00 AM UTC

CVE-2022-31152 - advisory for GHSA-jhjh-776m-4765

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Synapse from Matrix contain the following vulnerability:

Synapse is an open-source Matrix homeserver written and maintained by the Matrix.org Foundation. The Matrix specification specifies a list of [event authorization rules] (https://spec.matrix.org/v1.2/rooms/v9/#authorization-rules) which must be checked when determining if an event should be accepted into a room. In versions of Synapse up to and including version 1.61.0, some of these rules are not correctly applied. An attacker could craft events which would be accepted by Synapse but not a spec-conformant server, potentially causing divergence in the room state between servers. Administrators of homeservers with federation enabled are advised to upgrade to version 1.62.0 or higher. Federation can be disabled by setting [`federation_domain_whitelist`] (https://matrix-org.github.io/synapse/latest/usage/configuration/config_documentation.html#federation_domai to an empty list (`[]`) as a workaround.

CVE-2022-31152 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **matrix-org** - **synapse** version **< 1.62.0**

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	NONE	NONE	HIGH

CVE References

Description	Tags	Link

Fix inconsistencies in event validation for `m.room.create` events by richvdh · Pull Request #13087 · matrix-org/synapse · GitHub	github.com text/html	MISC github.com/matrix-org/synapse/pull/13087
Fix inconsistencies in event validation by richvdh · Pull Request #13088 · matrix-org/synapse · GitHub	github.com text/html	MISC github.com/matrix-org/synapse/pull/13088
Denial of service due to incorrect application of event authorization rules · Advisory · matrix-org/synapse · GitHub	github.com text/html	CONFIRM github.com/matrix-org/synapse/security/advisories/GHSA-jhjh-776m-4765
Release v1.62.0 · matrix-org/synapse · GitHub	github.com text/html	MISC github.com/matrix-org/synapse/releases/tag/v1.62.0

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	Matrix	Synapse	All	All	All	All

cpe:2.3:a:matrix:synapse:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31152 : Synapse is an open-source Matrix homeserver written and maintained by the Matrix.org… twitter.com/i/web/status/1…	2022-09-02 20:07:09
/r/netcve	CVE-2022-31152	2022-09-02 21:38:16

← 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 registred 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