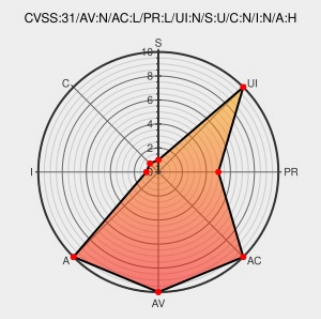
CVE-2020-26257

Published on: 12/09/2020 12:00:00 AM UTC

Last Modified on: 10/12/2022 02:01:00 PM UTC

CVE-2020-26257 - advisory for GHSA-hxmp-pqch-c8mm

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

Matrix is an ecosystem for open federated Instant Messaging and VoIP. Synapse is a reference "homeserver" implementation of Matrix. A malicious or poorly-implemented homeserver can inject malformed events into a room by specifying a different room id in the path of a `/send_join`, `/send_leave`, `/invite` or `/exchange_third_party_invite` request. This can lead to a denial of service in which future events will not be correctly sent to other servers over federation. This affects any server which accepts federation requests from untrusted servers. The Matrix Synapse reference implementation before version 1.23.1 the implementation is vulnerable to this injection attack. Issue is fixed in version 1.23.1. As a workaround homeserver administrators could limit access to the federation API to trusted servers (for example via `federation_domain_whitelist`).

CVE-2020-26257 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **matrix-org** - **synapse** version **< 1.23.1**

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality	**Integrity**	**Availability**

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Denial of service attack via incorrect parameters to federation APIs · Advisory · matrix-org/synapse · GitHub	Third Party Advisory, github.com, text/html	CONFIRM github.com/matrix-org/synapse/security/advisories/GHSA-hxmp-pqch-c8mm
Consistently use room_id from federation request body (#8776) · matrix-org/synapse@3ce2f30 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/matrix-org/synapse/commit/3ce2f303f15f6ac3dc352298972dc6e04d9b7a8b
[SECURITY] Fedora 33 Update: matrix-synapse-1.24.0-1.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org, text/html	FEDORA FEDORA-2020-eeb66c2ece
[SECURITY] Fedora 32 Update: matrix-synapse-1.24.0-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org, text/html	FEDORA FEDORA-2020-a2172c484d
Consistently use room_id from federation request body by richvdh · Pull Request #8776 · matrix-org/synapse · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/matrix-org/synapse/pull/8776
synapse/CHANGES.md at develop · matrix-org/synapse · GitHub	Release Notes, Third Party Advisory, github.com, text/html	MISC github.com/matrix-org/synapse/blob/develop/CHANGES.md#synapse-1231-2020-12-09

Related QID Numbers

501693 Alpine Linux Security Update for synapse

690432 Free Berkeley Software Distribution (FreeBSD) Security Update for py-matrix-synapse (cfa0be42-3cd7-11eb-9de7-641c67a117d8)

983225 Python (pip) Security Update for matrix-synapse (GHSA-hxmp-pqch-c8mm)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Matrix	Synapse	All	All	All	All
Application	Matrix	Synapse	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*

cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

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