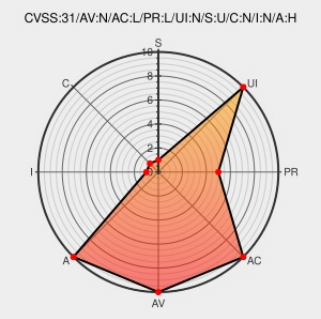
CVE-2022-31052

Published on: Not Yet Published

Last Modified on: 07/09/2022 12:15:00 AM UTC

CVE-2022-31052 - advisory for GHSA-22p3-qrh9-cx32

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

Synapse is an open source home server implementation for the Matrix chat network. In versions prior to 1.61.1 URL previews of some web pages can exhaust the available stack space for the Synapse process due to unbounded recursion. This is sometimes recoverable and leads to an error for the request causing the problem, but in other cases the Synapse process may crash altogether. It is possible to exploit this maliciously, either by malicious users on the homeserver, or by remote users sending URLs that a local user's client may automatically request a URL preview for. Remote users are not able to exploit this directly, because the URL preview endpoint is authenticated. Deployments with `url_preview_enabled: false` set in configuration are not affected. Deployments with `url_preview_enabled: true` set in configuration **are** affected. Deployments with no configuration value set for `url_preview_enabled` are not affected, because the default is `false`. Administrators of homeservers with URL previews enabled are advised to upgrade to v1.61.1 or higher. Users unable to upgrade should set `url_preview_enabled` to false.

CVE-2022-31052 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **matrix-org** - **synapse** version **< 1.61.1**

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: 3.5 - LOW

Access	Access	Authentication

Vector	Complexity	
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] Fedora 36 Update: matrix-synapse-1.61.1-1.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-45bf6d4b88
[SECURITY] Fedora 35 Update: matrix-synapse-1.61.1-1.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-1a2312e4d6
URL previews of unusual or maliciously-crafted pages can crash Synapse media repositories or Synapse monoliths · Advisory · matrix-org/synapse · GitHub	github.com text/html	CONFIRM github.com/matrix-org/synapse/security/advisories/GHSA-22p3-qrh9-cx32
Merge pull request from GHSA-22p3-qrh9-cx32 · matrix-org/synapse@fa13080 · GitHub	github.com text/html	MISC github.com/matrix-org/synapse/commit/fa1308061802ac7b7d20e954ba7372c5ac292333
Client-Server API | Matrix Specification	spec.matrix.org text/html	MISC spec.matrix.org/v1.2/client-server-api/#get_matrixmediav3preview_url

Related QID Numbers

282920 Fedora Security Update for matrix (FEDORA-2022-1a2312e4d6)

282921 Fedora Security Update for matrix (FEDORA-2022-45bf6d4b88)

502369 Alpine Linux Security Update for synapse

690888 Free Berkeley Software Distribution (FreeBSD) Security Update for py (07c0d782-f758-11ec-acaa-901b0e9408dc)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Matrix	Synapse	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:*:*

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31052 : Synapse is an open source home server implementation for the Matrix chat network. In versions prio… twitter.com/i/web/status/1…	2022-06-28 17:12:08
/r/netcve	CVE-2022-31052	2022-06-28 18:38:29

← Previous ID

Next ID→