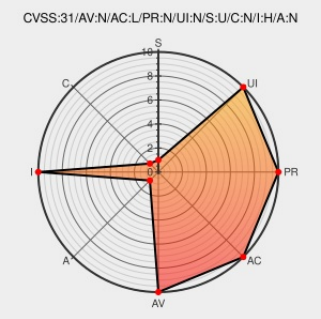
# CVE-2021-41281

Published on: Not Yet Published

Last Modified on: 11/29/2021 02:49:00 PM UTC

## **CVE-2021-41281** - advisory for GHSA-3hfw-x7gx-437c

Source: Mitre | Source: Nist | Print: PDF




Certain versions of Synapse from Matrix contain the following vulnerability:

Synapse is a package for Matrix homeservers written in Python 3/Twisted. Prior to version 1.47.1, Synapse instances with the media repository enabled can be tricked into downloading a file from a remote server into an arbitrary directory. No authentication is required for the affected endpoint. The last 2 directories and file name of the path are chosen randomly by Synapse and cannot be controlled by an attacker, which limits the impact. Homeservers with the media repository disabled are unaffected. Homeservers with a federation whitelist are also unaffected, since Synapse will check the remote hostname, including the trailing `../`s, against the whitelist. Server administrators should upgrade to 1.47.1 or later. Server administrators using a reverse proxy could, at the expense of losing media functionality, may block the certain endpoints as a workaround. Alternatively, non-containerized deployments can be adapted to use the hardened systemd config.

CVE-2021-41281 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **matrix-org** - **synapse** version **< 1.47.1**

### 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 | HIGH | NONE |

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |

| Confidentiality Impact | Integrity Impact | Availability Impact |
|---|---|---|
| NONE | PARTIAL | NONE |

## CVE References

| Description | Tags | Link |
|---|---|---|
| Prevent the media store from writing outside of the configured directory · matrix-org/synapse@91f2bd0 · GitHub | github.com text/html | MISC github.com/matrix-org/synapse/commit/91f2bd090 |
| Release v1.47.1 · matrix-org/synapse · GitHub | github.com text/html | MISC github.com/matrix-org/synapse/releases/tag/v1.47.1 |
| Path traversal when downloading remote media · Advisory · matrix-org/synapse · GitHub | github.com text/html | CONFIRM github.com/matrix-org/synapse/security/advisories/GHSA-3hfw-x7gx-437c |



## Related QID Numbers

690482 Free Berkeley Software Distribution (FreeBSD) Security Update for py-matrix-synapse (27aa2253-4c72-11ec-b6b9-e86a64caca56)

980024 Python (pip) Security Update for matrix-synapse (GHSA-3hfw-x7gx-437c)

## 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-2021-41281 : Synapse is a package for Matrix homeservers written in Python 3/Twisted. Prior to version 1.47.1,… twitter.com/i/web/status/1… | 2021-11-23 19:53:35 |
| @LinInfoSec | Python - CVE-2021-41281: github.com/matrix-org/syn… | 2021-11-23 21:36:15 |

← Previous ID

Next ID→

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**