



CVE-2023-42453

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

Summary

CVE	CVE-2023-42453
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-27 15:19:00 UTC
Updated	2024-01-07 11:15:00 UTC
Description	Synapse is an open-source Matrix homeserver written and maintained by the Matrix.org Foundation. Users were able to for

Risk And Classification

Problem Types: CWE-285

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Matrix	Synapse	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 39 Update: matrix-synapse-1.94.0-2.fc39 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
security.gentoo.org/glsa/202401-12		security.gentoo.org
[SECURITY] Fedora 37 Update: matrix-synapse-1.80.0-6.fc37 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
[SECURITY] Fedora 38 Update: matrix-synapse-1.93.0-2.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
Additional validation of receipts by clokep · Pull Request #16327 · matrix-org/synapse · GitHub	MISC	github.com
Improper validation of receipts allows forged read receipts · Advisory · matrix-org/synapse · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[284585](#) Fedora Security Update for matrix (FEDORA-2023-5d980e6aaf)

[284586](#) Fedora Security Update for matrix (FEDORA-2023-84ee781688)

[285204](#) Fedora Security Update for matrix (FEDORA-2023-4d4c73a8f0)

[503363](#) Alpine Linux Security Update for synapse

[506255](#) Alpine Linux Security Update for synapse

[710826](#) Gentoo Linux Synapse Multiple Vulnerabilities (GLSA 202401-12)

[995440](#) Python (Pip) Security Update for matrix-synapse (GHSA-7565-cq32-vx2x)

© [CVE.report](#) 2026 |

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 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)