CVE-2020-26891

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-26891
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-19 17:15:00 UTC
Updated	2020-10-26 21:30:00 UTC
Description	AuthRestServlet in Matrix Synapse before 1.21.0 is vulnerable to XSS due to unsafe interpolation of the session GET parar

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Matrix	Synapse	All	All	All	All
Application	Matrix	Synapse	All	All	All	All

References

Reference	Source	Link
Synapse 1.21.2 released, and security advisory. | Matrix.org	MISC	matrix.o
Release v1.21.2 · matrix-org/synapse · GitHub	MISC	github.c
Cross-site scripting (XSS) vulnerability in the fallback authentication endpoint · Advisory · matrix-org/synapse · GitHub	CONFIRM	github.c
Convert additional templates to Jinja by clokep · Pull Request #8444 · matrix-org/synapse · GitHub	MISC	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501692 Alpine Linux Security Update for synapse

690349 Free Berkeley Software Distribution (FreeBSD) Security Update for py-matrix-synapse (5f39d80f-107c-11eb-8b47-

641c67a117d8)

982971 Python (pip) Security Update for matrix-synapse (GHSA-3x8c-fmpc-5rmq)