CVE-2022-45197

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

Summary

CVE	CVE-2022-45197
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-25 05:15:00 UTC
Updated	2023-05-03 12:16:00 UTC
Description	Slixmpp before 1.8.3 lacks SSL Certificate hostname validation in XMLStream, allowing an attacker to pose as any server i

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Slixmpp Project	Slixmpp	All	All	All	All

References

Reference	Source	Link
slixmpp: Insufficient Certificate Validation (GLSA 202305-07) — Gentoo security	GENTOO	security.gentoo
Commits · master · poezio / slixmpp · GitLab	MISC	lab.louiz.org
CVE-2022-45197: Fix missing certificate hostname validation (b60b1b98) · Commits · poezio / slixmpp · GitLab	CONFIRM	lab.louiz.org
History for slixmpp/xmlstream/xmlstream.py - poezio/slixmpp · GitHub	MISC	github.com
Tags · poezio/slixmpp · 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

182739 Debian Security Update for slixmpp (CVE-2022-45197)

283351 Fedora Security Update for python (FEDORA-2022-20a2dbdd45)

283409 Fedora Security Update for python (FEDORA-2022-6720bd776b)

691132 Free Berkeley Software Distribution (FreeBSD) Security Update for py (93db4f92-9997-4f4f-8614-3963d9e2b0ec)

710716 Gentoo Linux slixmpp Insufficient Certificate Validation Vulnerability (GLSA 202305-07)

Free CVE JSON API cve.report/api

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