CVE-2019-1000021

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

Summary

CVE	CVE-2019-1000021
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-04 21:29:00 UTC
Updated	2023-11-07 03:02:00 UTC
Description	slixmpp version before commit 7cd73b594e8122dddf847953fcfc85ab4d316416 contains an incorrect Access Control vulner

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
[SECURITY] Fedora 30 Update: python-slixmpp-1.4.2-1.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraprojec
[SECURITY] Fedora 29 Update: python-slixmpp-1.4.2-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraprojec
XEP-0223: Fix default access_model, it MUST be whitelist. (7cd73b59) · Commits · poezio / slixmpp · GitLab	MISC	lab.louiz.org
XEP-0223: Private Information via Pubsub	MISC	xmpp.org
[SECURITY] Fedora 29 Update: python-slixmpp-1.4.2-1.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraprojec
[SECURITY] Fedora 30 Update: python-slixmpp-1.4.2-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraprojec
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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