



CVE-2022-39248

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

Summary

CVE	CVE-2022-39248
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-28 20:15:00 UTC
Updated	2022-09-30 16:24:00 UTC
Description	matrix-android-sdk2 is the Matrix SDK for Android. Prior to version 1.5.1, an attacker cooperating with a malicious homeser

Risk And Classification

Problem Types: CWE-287 | CWE-322

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Matrix	Software Development Kit	All	All	All	All

References

Reference	Source	Link
Olm/Megolm protocol confusion · Advisory · matrix-org/matrix-android-sdk2 · GitHub	CONFIRM	github.com
Release v1.5.1 · matrix-org/matrix-android-sdk2 · GitHub	MISC	github.com
Upgrade now to address E2EE vulnerabilities in matrix-js-sdk, matrix-ios-sdk and matrix-android-sdk2 Matrix.org	MISC	matrix.org
Merge branch 'release/1.5.1' into develop · matrix-org/matrix-android-sdk2@77df720 · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.or
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.

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