



CVE-2021-34813

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

Summary

CVE	CVE-2021-34813
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-16 18:15:00 UTC
Updated	2021-06-23 14:29:00 UTC
Description	Matrix libolm before 3.2.3 allows a malicious Matrix homeserver to crash a client (while it is attempting to retrieve an Olm er

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
3.2.3 · matrix-org / Olm · GitLab	MISC	gitlab.matrix.org	
Adventures in fuzzing libolm Matrix.org	MISC	matrix.org	
olm_pk_decrypt: Ensure inputs are of correct length. (ccc0d122) · Commits · matrix-org / Olm · GitLab	MISC	gitlab.matrix.org	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[182094](#) Debian Security Update for olm (CVE-2021-34813)

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](#).

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