



CVE-2022-20917

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-20917
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-15 03:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	A vulnerability in the Extensible Messaging and Presence Protocol (XMPP) message processing feature of Cisco Jabber cc

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Jabber	All	All	All	All
Application	Cisco	Jabber	All	All	All	All
Application	Cisco	Jabber	All	All	All	All
Application	Cisco	Jabber	All	All	All	All

References

Reference	Source	Link
Cisco Jabber Client Software Extensible Messaging and Presence Protocol Stanza Smuggling Vulnerability	MISC	sec.cloudapps.cisc
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

[317244](#) Cisco Jabber Client Software Extensible Messaging and Presence Protocol Stanza Smuggling Vulnerability (cisco-sa-jabber-xmpp-Ne9SCM)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)