



CVE-2020-24619

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

Summary

CVE	CVE-2020-24619
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-22 12:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	In mainwindow.cpp in Shotcut before 20.09.13, the upgrade check misuses TLS because of setPeerVerifyMode(QSslSocket::VerifyMode::VerifyNone) which disables TLS verification. This allows an attacker to impersonate the Shotcut server and trick the client into downloading a malicious update.

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Melttech	Shotcut	All	All	All	All
Application	Melttech	Shotcut	All	All	All	All

References

Reference	Source	Link	Tags
fix upgrade check is not using TLS correctly · mltframework/shotcut@f008adc · GitHub	MISC	github.com	Patch, Third Party Advis
Shotcut - New Version 20.09.13: Pad Blur and Rich Text Video Filters	CONFIRM	shotcut.org	Release Notes, Vendor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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