



CVE-2017-12194

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

Summary

CVE	CVE-2017-12194
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-14 21:29:00 UTC
Updated	2019-06-17 13:49:00 UTC
Description	A flaw was found in the way spice-client processed certain messages sent from the server. An attacker, having control of m

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spice-gtk Project	Spice-gtk	All	All	All	All

References

Reference	Source	Link
spice-gtk: Remote code execution (GLSA 201811-20) — Gentoo security	GENTOO	security.g
spice-gtk CVE-2017-12194 Integer Overflow Vulnerability	BID	www.secu
USN-3659-1: Spice vulnerability Ubuntu security notices Ubuntu	UBUNTU	usn.ubunt
1501200 – (CVE-2017-12194) CVE-2017-12194 spice-gtk: Integer overflows causing buffer overflows in spice-client	CONFIRM	bugzilla.re
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710210 Gentoo Linux spice-gtk Remote code execution Vulnerability (GLSA 201811-20)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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