



CVE-2021-20201

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

Summary

CVE	CVE-2021-20201
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-28 11:15:00 UTC
Updated	2022-10-21 20:02:00 UTC
Description	A flaw was found in spice in versions before 0.14.92. A DoS tool might make it easier for remote attackers to cause a denial of service (CPU consumption) by sending a large number of renegotiation requests.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Spice Project	Spice	All	All	All	All

References

Reference	Source	Link	Tags
TLS Renegotiation and Denial of Service Attacks Qualys Security Blog	MISC	blog.qualys.com	
1921846 – (CVE-2021-20201) CVE-2021-20201 spice: Client initiated renegotiation denial of service	MISC	bugzilla.redhat.com	
Spice Server: Multiple Vulnerabilities (GLSA 202208-10) — Gentoo security	GENTOO	security.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159228](#) Oracle Enterprise Linux Security Update for spice (ELSA-2021-1924)

180135 Debian Security Update for spice (CVE-2021-20201)
239288 Red Hat Update for spice (RHSA-2021:1924)
500650 Alpine Linux Security Update for spice
504417 Alpine Linux Security Update for spice
670591 EulerOS Security Update for spice (EulerOS-SA-2021-2349)
670693 EulerOS Security Update for spice (EulerOS-SA-2021-2451)
671046 EulerOS Security Update for spice (EulerOS-SA-2021-2616)
710583 Gentoo Linux Spice Server Multiple Vulnerabilities (GLSA 202208-10)
750133 SUSE Enterprise Linux Security Update for spice (SUSE-SU-2021:1901-1)
750134 SUSE Enterprise Linux Security Update for spice (SUSE-SU-2021:1906-1)
750144 SUSE Enterprise Linux Security Update for spice (SUSE-SU-2021:1927-1)
750157 SUSE Enterprise Linux Security Update for spice (SUSE-SU-2021:1956-1)
750646 OpenSUSE Security Update for spice (openSUSE-SU-2021:0874-1)
753102 SUSE Enterprise Linux Security Update for spice (SUSE-SU-2022:2881-1)
940010 AlmaLinux Security Update for spice (ALSA-2021:1924)
960452 Rocky Linux Security Update for spice (RLSA-2021:1924)

© [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](#)