



CVE-2020-25653

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

Summary

CVE	CVE-2020-25653
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-26 02:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	A race condition vulnerability was found in the way the spice-vdagentd daemon handled new client connections. This flaw n

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Spice-space	Spice-vdagent	All	All	All	All

References

Reference
[SECURITY] Fedora 32 Update: spice-vdagent-0.21.0-1.fc32 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 33 Update: spice-vdagent-0.21.0-1.fc33 - package-announce - Fedora Mailing-Lists
oss-security - Security Issues in the spice-vdagentd daemon
[SECURITY] Fedora 33 Update: spice-vdagent-0.21.0-1.fc33 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 32 Update: spice-vdagent-0.21.0-1.fc32 - package-announce - Fedora Mailing-Lists
1886372 – (CVE-2020-25653) CVE-2020-25653 spice-vdagent: UNIX domain socket peer PID retrieved via `SO_PEERCRE` is subject to ra
[SECURITY] [DLA 2524-1] spice-vdagent security update

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159216	Oracle Enterprise Linux Security Update for spice-vdagent (ELSA-2021-1791)
239302	Red Hat Update for spice-vdagent (RHSA-2021:1791)
377381	Alibaba Cloud Linux Security Update for spice-vdagent (ALINUX3-SA-2022:0084)
670499	EulerOS Security Update for spice-vdagent (EulerOS-SA-2021-2257)
670525	EulerOS Security Update for spice-vdagent (EulerOS-SA-2021-2283)
670557	EulerOS Security Update for spice-vdagent (EulerOS-SA-2021-2316)
670592	EulerOS Security Update for spice-vdagent (EulerOS-SA-2021-2350)
670694	EulerOS Security Update for spice-vdagent (EulerOS-SA-2021-2452)
670962	EulerOS Security Update for spice-vdagent (EulerOS-SA-2021-2617)
750925	OpenSUSE Security Update for spice-vdagent (openSUSE-SU-2021:2614-1)
750974	SUSE Enterprise Linux Security Update for spice-vdagent (SUSE-SU-2021:2766-1)
750989	SUSE Enterprise Linux Security Update for spice-vdagent (SUSE-SU-2021:2803-1)
901471	Common Base Linux Mariner (CBL-Mariner) Security Update for spice-vdagent (7365-1)
940204	AlmaLinux Security Update for spice-vdagent (ALSA-2021:1791)
960751	Rocky Linux Security Update for spice-vdagent (RLSA-2021:1791)

© [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](#)