



CVE-2021-20181

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

Summary

CVE	CVE-2021-20181
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-13 16:15:00 UTC
Updated	2023-11-07 03:28:00 UTC
Description	A race condition flaw was found in the 9pfs server implementation of QEMU up to and including 5.2.0. This flaw allows a ma

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	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link
1927007 – (CVE-2021-20181) CVE-2021-20181 qemu: 9pfs: TOCTOU privilege escalation vulnerability	MISC	bugzilla.redhat.com
[SECURITY] [DLA 3099-1] qemu security update	MLIST	lists.debian.org
[SECURITY] [DLA 2560-1] qemu security update	MLIST	lists.debian.org
ZDI-21-159 Zero Day Initiative	MISC	www.zerodayinitiative.
CVE-2021-20181 QEMU Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
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

174921 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1245-1)
174922 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1240-1)
174923 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1241-1)
174924 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1244-1)
174926 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1242-1)
179892 Debian Security Update for qemu (CVE-2021-20181)
180995 Debian Security Update for qemu (DLA 3099-1)
502354 Alpine Linux Security Update for qemu
671198 EulerOS Security Update for qemu (EulerOS-SA-2022-1034)
671203 EulerOS Security Update for qemu (EulerOS-SA-2022-1014)
750338 OpenSUSE Security Update for qemu (openSUSE-SU-2021:0363-1)
900156 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
902810 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (4271)

© [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](#)