



CVE-2019-20382

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

Summary

CVE	CVE-2019-20382
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-05 19:15:00 UTC
Updated	2023-11-07 03:09:00 UTC
Description	QEMU 4.1.0 has a memory leak in zrle_compress_data in ui/vnc-enc-zrle.c during a VNC disconnect operation because lib

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Qemu	Qemu	4.1.0	All	All	All
Application	Qemu	Qemu	4.1.0	All	All	All

References

Reference	Source	Link	Tags
git.qemu.org Git - qemu.git/commit	MISC	git.qemu.org	Patch, Third Party Advice
[SECURITY] [DLA 2288-1] qemu security update	MLIST	lists.debian.org	
USN-4372-1: QEMU vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
git.qemu.org Git - qemu.git/commit		git.qemu.org	

Debian -- Security Information -- DSA-4665-1 qemu	DEBIAN	www.debian.org	
oss-security - CVE-2019-20382 QEMU: vnc: memory leakage upon disconnect	MISC	www.openwall.com	Mailing List, Patch, Third
[security-announce] openSUSE-SU-2020:0468-1: important: Security update	SUSE	lists.opensuse.org	Third Party Advisory
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.

Legacy QID Mappings

[940423](#) AlmaLinux Security Update for virt:rhel (ALSA-2020:2774)

[960750](#) Rocky Linux Security Update for virt:rhel (RLSA-2020:2774)

© [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