CVE-2023-3255

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-3255
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-13 17:15:00 UTC
Updated	2023-11-07 04:18:00 UTC
Description	A flaw was found in the QEMU built-in VNC server while processing ClientCutText messages. A wrong exit condition may le

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Source	Link
2218486 – (CVE-2023-3255) CVE-2023-3255 QEMU: VNC: infinite loop in inflate_buffer() leads to denial of service	MISC	bugzilla.red
September 2023 QEMU Vulnerabilities in NetApp Products | NetApp Product Security	MISC	security.ne
cve-details	MISC	access.red
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160960 Oracle Enterprise Linux Security Update for kvm_utils3 (ELSA-2023-12855)

© 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 registred 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