



CVE-2017-15124

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

Summary

CVE	CVE-2017-15124
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-09 21:29:00 UTC
Updated	2023-02-12 23:28:00 UTC
Description	VNC server implementation in Quick Emulator (QEMU) 2.11.0 and older was found to be vulnerable to an unbounded mem

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All

References

Reference	S
Red Hat Customer Portal	R
USN-3575-1: QEMU vulnerabilities Ubuntu security notices	U
Red Hat Customer Portal	R
Red Hat Customer Portal	R
CVE-2017-15124 - Red Hat Customer Portal	M
1525195 – (CVE-2017-15124) CVE-2017-15124 Qemu: memory exhaustion through framebuffer update request message in VNC server	C
Debian -- Security Information -- DSA-4213-1 qemu	D
Red Hat Customer Portal	R
QEMU CVE-2017-15124 Denial of Service Vulnerability	B
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)