



CVE-2017-15118

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

Summary

CVE	CVE-2017-15118
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-27 21:29:00 UTC
Updated	2023-11-07 02:39:00 UTC
Description	A stack-based buffer overflow vulnerability was found in NBD server implementation in qemu before 2.11 allowing a client to

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

References

Reference	Source
oss-security - CVE-2017-15118 Qemu: stack buffer overflow in NBD server triggered via long export name	MISC
[Qemu-devel] [PULL 2/2] nbd/server: CVE-2017-15118 Stack smash on large	MISC
QEMU - NBD Server Long Export Name Stack Buffer Overflow - Linux dos Exploit	EXPLOIT-DB
Red Hat Customer Portal	REDHAT

QEMU 'b/nbd/server.c' Stack Buffer Overflow Vulnerability	BID
USN-3575-1: QEMU vulnerabilities Ubuntu security notices	UBUNTU
1516922 – (CVE-2017-15118) CVE-2017-15118 Qemu: stack buffer overflow in NBD server triggered via long export name	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
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](#)