



CVE-2018-18438

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

Summary

CVE	CVE-2018-18438
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-19 22:29:00 UTC
Updated	2021-08-04 17:15:00 UTC
Description	Qemu has integer overflows because IOReadHandler and its associated functions use a signed integer data type for a size

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	-	All	All	All
Application	Qemu	Qemu	-	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	12	All	All	All
Application	Redhat	Openstack	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	8	All	All	All
Application	Redhat	Openstack	8.0	All	All	All
Application	Redhat	Openstack	9	All	All	All
Application	Redhat	Openstack	9.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	12	All	All	All
Application	Redhat	Openstack	13.0	All	All	All

Application	Redhat	Openstack	8.0	All	All	All
Application	Redhat	Openstack	9.0	All	All	All

References

Reference	Source	Link
[Qemu-devel] [PATCH v2 07/11] chardev: Let IOReadHandler use unsigned ty	MLIST	lists.gnu.org
Malformed Request	BID	www.securityfocus.com/bid
oss-security - CVE-2018-18438 Qemu: Integer overflow in ccid_card_vscard_read() allows memory corruption	MLIST	www.openwall.com
[Qemu-devel] [PATCH v2 00/11] chardev: Convert IO handlers to use unsign	MLIST	lists.gnu.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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