



CVE-2017-8380

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

Summary

CVE	CVE-2017-8380
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-28 15:29:00 UTC
Updated	2017-09-06 02:06:00 UTC
Description	Buffer overflow in the "megasas_mmio_write" function in Qemu 2.9.0 allows remote attackers to have unspecified impact vi

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	2.9.0	All	All	All
Application	Qemu	Qemu	2.9.0	All	All	All

References

Reference	Source	Link	Tags
[Qemu-devel] [PATCH] scsi: avoid an off-by-one error in megasas_mmio_wri	CONFIRM	lists.gnu.org	Patch, Third Party Advi
QEMU 'megasas_mmio_write()' Function Out-of-Bounds Read Vulnerability	BID	www.securityfocus.com	Third Party Advisory, V
QEMU: Multiple vulnerabilities (GLSA 201706-03) — Gentoo security	GENTOO	security.gentoo.org	Issue Tracking, Third P
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

[710528](#) Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201706-03)

© [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](#)