CVE-2017-5856

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-5856
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-16 15:59:00 UTC
Updated	2023-02-12 23:29:00 UTC
Description	Memory leak in the megasas_handle_dcmd function in hw/scsi/megasas.c in QEMU (aka Quick Emulator) allows local gues

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link
git.qemu.org Git - qemu.git/commit	MISC	git.qemu-project.org
git.qemu.org Git - qemu.git/commit	CONFIRM	git.qemu-project.org
QEMU: Multiple vulnerabilities (GLSA 201702-28) — Gentoo Security	GENTOO	security.gentoo.org
[SECURITY] [DLA 1497-1] qemu security update	MLIST	lists.debian.org
Bug 1418342 – CVE-2017-5856 Qemu: scsi: megasas: host memory leakage in megasas_handle_dcmd	CONFIRM	bugzilla.redhat.com
oss-security - CVE request Qemu: scsi: megasas: host memory leakage in megasas_handle_dcmd	MLIST	www.openwall.com
oss-security - Re: CVE request Qemu: scsi: megasas: host memory leakage in megasas_handle_dcmd	MLIST	www.openwall.com
QEMU 'hw/scsi/megasas.c' Denial of Service Vulnerability	BID	www.securityfocus.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501229 Alpine Linux Security Update for qemu

505339 Alpine Linux Security Update for qemu

710393 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201702-28)

900063 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0