CVE-2016-5105

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-5105
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-02 14:59:02 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The megasas_dcmd_cfg_read function in hw/scsi/megasas.c in QEMU, when built with MegaRAID SAS 8708EM2 Host Bu

Risk And Classification

Primary CVSS: v3.1 4.4 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

EPSS: 0.000720000 probability, percentile 0.217110000 (date 2026-05-08)

Problem Types: CWE-908 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	1.9		AV:L/AC:M/Au:N/C:P/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
High

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
None

Availability

None

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:L/AC:M/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	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	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
[SECURITY] [DLA 1599-1] qemu security update	af854a3a-2127-422b-91ae-36
oss-security - Re: CVE Request Qemu: scsi: megasas: stack information leakage while reading configuration	af854a3a-2127-422b-91ae-36
USN-3047-2: QEMU regression | Ubuntu	af854a3a-2127-422b-91ae-36
[Qemu-devel] [PATCH v2] scsi: megasas: initialise local configuration da	af854a3a-2127-422b-91ae-36
oss-security - CVE Request Qemu: scsi: megasas: stack information leakage while reading configuration	af854a3a-2127-422b-91ae-36

Bug 1339583 – CVE-2016-5105 Qemu: scsi: megasas: stack information leakage while reading configuration	af854a3a-2127-422b-91ae-36
USN-3047-1: QEMU vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-36
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.