CVE-2014-2894

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

Summary

CVE	CVE-2014-2894
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-23 15:55:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Off-by-one error in the cmd_smart function in the smart self test in hw/ide/core.c in QEMU before 2.0 allows local users to h

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

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

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	0.1.0	All	All	All

Application	Qemu	Qemu	0.1.1	All	All	All
Application	Qemu	Qemu	0.1.2	All	All	All
Application	Qemu	Qemu	0.1.3	All	All	All
Application	Qemu	Qemu	0.1.4	All	All	All
Application	Qemu	Qemu	0.1.5	All	All	All
Application	Qemu	Qemu	0.1.6	All	All	All
Application	Qemu	Qemu	0.10.0	All	All	All
Application	Qemu	Qemu	0.10.1	All	All	All
Application	Qemu	Qemu	0.10.2	All	All	All
Application	Qemu	Qemu	0.10.3	All	All	All
Application	Qemu	Qemu	0.10.4	All	All	All
Application	Qemu	Qemu	0.10.5	All	All	All
Application	Qemu	Qemu	0.10.6	All	All	All
Application	Qemu	Qemu	0.11.0	All	All	All
Application	Qemu	Qemu	0.11.0	rc0	All	All
Application	Qemu	Qemu	0.11.0	rc1	All	All
Application	Qemu	Qemu	0.11.0	rc2	All	All
Application	Qemu	Qemu	0.11.0-rc0	All	All	All
Application	Qemu	Qemu	0.11.0-rc1	All	All	All
Application	Qemu	Qemu	0.11.0-rc2	All	All	All
Application	Qemu	Qemu	0.11.1	All	All	All
Application	Qemu	Qemu	0.12.0	All	All	All
Application	Qemu	Qemu	0.12.0	rc1	All	All
Application	Qemu	Qemu	0.12.0	rc2	All	All
Application	Qemu	Qemu	0.12.1	All	All	All
Application	Qemu	Qemu	0.12.2	All	All	All
Application	Qemu	Qemu	0.12.3	All	All	All
Application	Qemu	Qemu	0.12.4	All	All	All
Application	Qemu	Qemu	0.12.5	All	All	All
Application	Qemu	Qemu	0.13.0	All	All	All
Application	Qemu	Qemu	0.13.0	rc0	All	All
Application	Qemu	Qemu	0.13.0	rc1	All	All
Application	Qemu	Qemu	0.14.0	All	All	All
Application	Qemu	Qemu	0.14.0	rc0	All	All
Application	Qemu	Qemu	0.14.0	rc1	All	All
Application	Qemu	Qemu	0.14.0	rc2	All	All

Application	Qemu	Qemu	0.14.1	All	All	All
Application	Qemu	Qemu	0.15.0	rc1	All	All
Application	Qemu	Qemu	0.15.0	rc2	All	All
Application	Qemu	Qemu	0.15.1	All	All	All
Application	Qemu	Qemu	0.15.2	All	All	All
Application	Qemu	Qemu	0.2.0	All	All	All
Application	Qemu	Qemu	0.3.0	All	All	All
Application	Qemu	Qemu	0.4.0	All	All	All
Application	Qemu	Qemu	0.4.1	All	All	All
Application	Qemu	Qemu	0.4.2	All	All	All
Application	Qemu	Qemu	0.4.3	All	All	All
Application	Qemu	Qemu	0.5.0	All	All	All
Application	Qemu	Qemu	0.5.1	All	All	All
Application	Qemu	Qemu	0.5.2	All	All	All
Application	Qemu	Qemu	0.5.3	All	All	All
Application	Qemu	Qemu	0.5.4	All	All	All
Application	Qemu	Qemu	0.5.5	All	All	All
Application	Qemu	Qemu	0.6.0	All	All	All
Application	Qemu	Qemu	0.6.1	All	All	All
Application	Qemu	Qemu	0.7.0	All	All	All
Application	Qemu	Qemu	0.7.1	All	All	All
Application	Qemu	Qemu	0.7.2	All	All	All
Application	Qemu	Qemu	0.8.0	All	All	All
Application	Qemu	Qemu	0.8.1	All	All	All
Application	Qemu	Qemu	0.8.2	All	All	All
Application	Qemu	Qemu	0.9.0	All	All	All
Application	Qemu	Qemu	0.9.1	All	All	All
Application	Qemu	Qemu	0.9.1-5	All	All	All
Application	Qemu	Qemu	1.0	All	All	All
Application	Qemu	Qemu	1.0	rc1	All	All
Application	Qemu	Qemu	1.0	rc2	All	All
Application	Qemu	Qemu	1.0	rc3	All	All
Application	Qemu	Qemu	1.0	rc4	All	All
Application	Qemu	Qemu	1.0.1	All	All	All
Application	Qemu	Qemu	1.1	All	All	All

Application	Qemu	Qemu	1.1	rc1	All	All
Application	Qemu	Qemu	1.1	rc2	All	All
Application	Qemu	Qemu	1.1	rc3	All	All
Application	Qemu	Qemu	1.1	rc4	All	All
Application	Qemu	Qemu	1.1.1	All	All	All
Application	Qemu	Qemu	1.1.2	All	All	All
Application	Qemu	Qemu	1.2.0	All	All	All
Application	Qemu	Qemu	1.2.0	rc0	All	All
Application	Qemu	Qemu	1.2.0	rc1	All	All
Application	Qemu	Qemu	1.2.0	rc2	All	All
Application	Qemu	Qemu	1.2.0	rc3	All	All
Application	Qemu	Qemu	1.2.1	All	All	All
Application	Qemu	Qemu	1.2.2	All	All	All
Application	Qemu	Qemu	1.3.0	All	All	All
Application	Qemu	Qemu	1.3.0	rc0	All	All
Application	Qemu	Qemu	1.3.0	rc1	All	All
Application	Qemu	Qemu	1.3.0	rc2	All	All
Application	Qemu	Qemu	1.3.1	All	All	All
Application	Qemu	Qemu	1.4.0	rc0	All	All
Application	Qemu	Qemu	1.4.0	rc1	All	All
Application	Qemu	Qemu	1.4.1	All	All	All
Application	Qemu	Qemu	1.4.2	All	All	All
Application	Qemu	Qemu	1.5.0	All	All	All
Application	Qemu	Qemu	1.5.0	rc1	All	All
Application	Qemu	Qemu	1.5.0	rc2	All	All
Application	Qemu	Qemu	1.5.0	rc3	All	All
Application	Qemu	Qemu	1.5.1	All	All	All
Application	Qemu	Qemu	1.5.2	All	All	All
Application	Qemu	Qemu	1.5.3	All	All	All
Application	Qemu	Qemu	1.6.0	All	All	All
Application	Qemu	Qemu	1.6.0	rc1	All	All
Application	Qemu	Qemu	1.6.0	rc2	All	All
Application	Qemu	Qemu	1.6.0	rc3	All	All
Application	Qemu	Qemu	1.6.1	All	All	All
Application	Qemu	Qemu	1.6.2	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
[Qemu-devel] [PATCH for 2.0] ide: Correct improper smart self test count	af854a3a-2127-422b-91a
Security Advisory SA57945 - Qemu IDE SMART EXECUTE OFFLINE Memory Corruption Vulnerability - Secunia	af854a3a-2127-422b-91a
QEMU IDE SMART Out of Bounds Local Privilege Escalation Vulnerability	af854a3a-2127-422b-91a
Re: [Qemu-devel] [PATCH for 2.0] ide: Correct improper smart self test c	af854a3a-2127-422b-91a
Re: [Qemu-devel] [PATCH for 2.0] ide: Correct improper smart self test c	af854a3a-2127-422b-91a
oss-security - CVE request Qemu: out of bounds buffer access, guest triggerable via IDE SMART	af854a3a-2127-422b-91a
Red Hat Customer Portal	af854a3a-2127-422b-91a
USN-2182-1: QEMU vulnerabilities | Ubuntu	af854a3a-2127-422b-91a
oss-security - Re: CVE request Qemu: out of bounds buffer access, guest triggerable via IDE SMART	af854a3a-2127-422b-91a
Red Hat Customer Portal	af854a3a-2127-422b-91a
Red Hat Customer Portal	af854a3a-2127-422b-91a
Security Advisory SA58191 - Ubuntu update for qemu - Secunia	af854a3a-2127-422b-91a
Red Hat Customer Portal	MITRE
Red Hat Customer Portal	MITRE
Red Hat Customer Portal	MITRE
Red Hat Customer Portal	MITRE
Red Hat Customer Portal	MITRE
access.redhat.com | CVE-2014-2894	MITRE
Bug 1087971 – CVE-2014-2894 QEMU: out of bounds buffer accesses, guest triggerable via IDE SMART	MITRE
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report