CVE-2011-4111

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

Summary

CVE	CVE-2011-4111
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-26 15:55:08 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Buffer overflow in the ccid_card_vscard_handle_message function in hw/ccid-card-passthru.c in QEMU before 0.15.2 and 1

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

EPSS: 0.007950000 probability, percentile 0.740480000 (date 2026-05-05)

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

High

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:A/AC:H/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	0.15.0	All	All	All
Application	Qemu	Qemu	0.15.0	rc1	All	All
Application	Qemu	Qemu	0.15.0	rc2	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	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	6.1.z	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
access.redhat.com	af854a3a-2127-422b-91ae-364
751310 – (CVE-2011-4111) CVE-2011-4111 qemu: ccid: buffer overflow in handling of VSC_ATR message	af854a3a-2127-422b-91ae-364
git.qemu.org Git - qemu.git/log	af854a3a-2127-422b-91ae-364
access.redhat.com	af854a3a-2127-422b-91ae-364
git.qemu.org Git - qemu-stable-0.15.git/log	af854a3a-2127-422b-91ae-364
git.qemu.org Git - qemu-stable-0.15.git/log	MITRE
git.qemu.org Git - qemu.git/log	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**