Qemu: sdhci: heap buffer overflow in sdhci_write_dataport()

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

Summary

CVE	CVE-2024-3447
State	PUBLISHED
Assigner	fedora
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-11-14 12:15:17 UTC
Updated	2026-05-12 12:16:57 UTC
Description	A heap-based buffer overflow was found in the SDHCI device emulation of QEMU. The bug is triggered when both `s->data

Risk And Classification

Primary CVSS: v3.1 6 MEDIUM from patrick@puiterwijk.org

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

Problem Types: CWE-122 | CWE-122 Heap-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	patrick@puiterwijk.org	Secondary	6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H
3.1	CNA	CVSS	6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
High

User Interaction
None

Scope
Changed

Confidentiality
None

Integrity
None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8 Advanced Virtualization	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified
ADP	Siemens	RUGGEDCOM ROX MX5000	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX MX5000RE	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1400	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1500	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1501	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1510	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1511	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1512	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1524	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX1536	affected V2.17.1 custom	Not specified
ADP	Siemens	RUGGEDCOM ROX RX5000	affected V2.17.1 custom	Not specified

References

Reference	Source	Link	T
bugzilla.redhat.com/show_bug.cgi	patrick@puiterwijk.org	bugzilla.redhat.com	Is
access.redhat.com/security/cve/CVE-2024-3447	patrick@puiterwijk.org	access.redhat.com	T
cert-portal.siemens.com/productcert/html/ssa-577017.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
security.netapp.com/advisory/ntap-20250425-0005	af854a3a-2127-422b-91ae-364da2661108	security.netapp.com	V
bugs.chromium.org/p/oss-fuzz/issues/detail	patrick@puiterwijk.org	bugs.chromium.org	E
lists.debian.org/debian-lts-announce/2025/04/msg00042.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	

patchew.org/QEMU/20240404085549.16987-1-philmd@linaro.org	patrick@puiterwijk.org	patchew.org	B
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Chuhong Yuan for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-04-09T00:00:00.000Z	Reported to Red Hat.
CNA	2024-04-04T00:00:00.000Z	Made public.

There are currently no legacy QID mappings associated with this CVE.