CVE-2017-13711

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

Summary

CVE	CVE-2017-13711
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-01 13:29:00 UTC
Updated	2020-10-29 17:24:00 UTC
Description	Use-after-free vulnerability in the sofree function in slirp/socket.c in QEMU (aka Quick Emulator) allows attackers to cause a

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	access.redhat.com
Debian -- Security Information -- DSA-3991-1 qemu	DEBIAN	www.debian.org
oss-security - CVE-2017-13711 Qemu: Slirp: use-after-free when sending response	MLIST	www.openwall.com
QEMU CVE-2017-13711 Denial of Service Vulnerability	BID	www.securityfocus.com
1486400 – (CVE-2017-13711) CVE-2017-13711 QEMU: Slirp: use-after-free when sending response	CONFIRM	bugzilla.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
[Qemu-devel] [PATCH] slirp: fix clearing ifq_so from pending packets	MLIST	lists.gnu.org
Red Hat Customer Portal	REDHAT	access.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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**