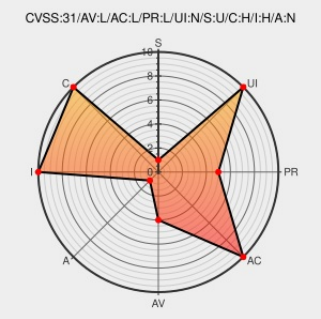
CVE-2015-8743

Published on: 12/29/2016 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:11 AM UTC

CVE-2015-8743

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

QEMU (aka Quick Emulator) built with the NE2000 device emulation support is vulnerable to an OOB r/w access issue. It could occur while performing 'ioport' r/w operations. A privileged (CAP_SYS_RAWIO) user/process could use this flaw to leak or corrupt QEMU memory bytes.

CVE-2015-8743 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: 3.6 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
oss-security - Re: CVE request Qemu: net: ne2000: OOB r/w in ioport operations	Mailing List Third Party Advisory www.openwall.com	MLIST [oss-security] 20160104 Re: CVE request Qemu: net: ne2000: OOB r/w in ioport operations

	text/html	
oss-security - CVE request Qemu: net: ne2000: OOB r/w in ioport operations	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160104 CVE request Qemu: net: ne2000: OOB r/w in ioport operations
Debian -- Security Information -- DSA-3471-1 qemu	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3471
Debian -- Security Information -- DSA-3469-1 qemu	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3469
Bug 1264929 – CVE-2015-8743 Qemu: net: ne2000: OOB memory access in ioport r/w functions	Issue Tracking bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1264929
Debian -- Security Information -- DSA-3470-1 qemu-kvm	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3470
QEMU NE2000 Memory Access Error Lets Local Users Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1034574
QEMU CVE-2015-8743 Information Disclosure Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 79820
Re: [Qemu-devel] [PATCH v3] net: ne2000: fix bounds check in ioport oper	Patch Vendor Advisory lists.gnu.org text/html	MLIST [qemu-devel] 20160104 Re: [PATCH v3] net: ne2000: fix bounds check in ioport operations
QEMU: Multiple vulnerabilities (GLSA 201602-01) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201602-01

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All

Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→