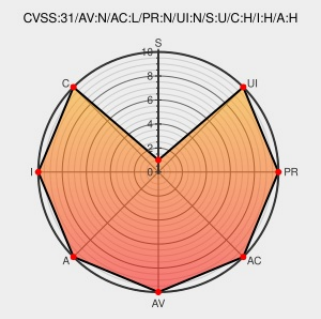
CVE-2016-7161

Published on: 10/05/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:05 PM UTC

CVE-2016-7161

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



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

Heap-based buffer overflow in the .receive callback of xlnx.xps-ethernetlite in QEMU (aka Quick Emulator) allows attackers to execute arbitrary code on the QEMU host via a large ethlite packet.

CVE-2016-7161 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
[SECURITY] [DLA 1599-1] qemu security update	Third Party Advisory, lists.debian.org, text/html	MLIST [debian-lts-announce] 20181130 [SECURITY] [DLA 1599-1] qemu security update
oss-security - Re: CVE request Qemu: hw:	Mailing List	MLIST [oss-security] 20160923 Re: CVE request Qemu: hw: net: Fix

net: Fix a heap overflow in xlnx.xps-ethernetlite	Third Party Advisory www.openwall.com text/html	a heap overflow in xlnx.xps-ethernetlite
QEMU: Multiple vulnerabilities (GLSA 201611-11) — Gentoo Security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201611-11
Re: [Qemu-devel] [PULL 3/3] hw/net: Fix a heap overflow in xlnx.xps-ethe	Mailing List Patch Vendor Advisory lists.gnu.org text/html	MLIST [qemu-devel] 20160809 [PULL 3/3] hw/net: Fix a heap overflow in xlnx.xps-ethernetlite
QEMU 'xilinx_ethlite.c' Heap Based Buffer Overflow Vulnerability	Broken Link Third Party Advisory VDB Entry cve.report (archive) text/html	BID 93141
openSUSE-SU-2016:3237-1: moderate: Security update for qemu	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:3237
Re: [Qemu-devel] [PATCH] hw/net: Fix a heap overflow in xlnx.xps-etherne	Mailing List Patch Vendor Advisory lists.gnu.org text/x-diff	MLIST [qemu-devel] 20160809 [PATCH] hw/net: Fix a heap overflow in xlnx.xps-ethernetlite
git.qemu.org Git - qemu.git/commit	Issue Tracking Patch git.qemu.org text/xml	CONFIRM git.qemu.org/?p=qemu.git;a=commit;h=a0d1cbdacff5df4ded16b753b38fdd9da6092968
oss-security - CVE request Qemu: hw: net: Fix a heap overflow in xlnx.xps-ethernetlite	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160923 CVE request Qemu: hw: net: Fix a heap overflow in xlnx.xps-ethernetlite

Related QID Numbers

900010 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

903207 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (3543)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	2.7.0	rc0	All	All

Application	Qemu	Qemu	2.7.0	rc1	All	All
Application	Qemu	Qemu	2.7.0	rc2	All	All
Application	Qemu	Qemu	2.7.0	rc0	All	All
Application	Qemu	Qemu	2.7.0	rc1	All	All
Application	Qemu	Qemu	2.7.0	rc2	All	All
Application	Qemu	Qemu	All	All	All	All

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

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

cpe:2.3:a:qemu:qemu:2.7.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.7.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.7.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.7.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.7.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.7.0:rc2:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→