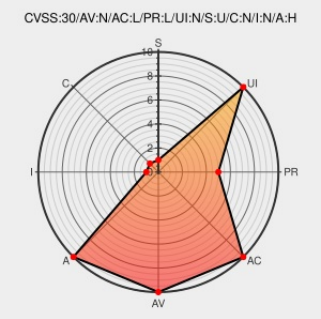
CVE-2018-10839

Published on: 10/16/2018 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:50:00 AM UTC

CVE-2018-10839

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Qemu emulator <= 3.0.0 built with the NE2000 NIC emulation support is vulnerable to an integer overflow, which could lead to buffer overflow issue. It could occur when receiving packets over the network. A user inside guest could use this flaw to crash the Qemu process resulting in DoS.

CVE-2018-10839 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **The QEMU Project** - **Qemu-kvm** version **= <= 3.0.0**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2018-10839 - Red Hat Customer Portal	access.redhat.com	MISC access.redhat.com/security/cve/CVE-

	text/html	2018-10839
[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
[Qemu-devel] [PULL 21/25] ne2000: fix possible out of bound access in ne	Exploit Mailing List Third Party Advisory lists.gnu.org text/x-diff	MLIST [qemu-devel] 20180926 [PULL 21/25] ne2000: fix possible out of bound access in ne2000_receive
1581013 – (CVE-2018-10839) CVE-2018-10839 QEMU: ne2000: integer overflow leads to buffer overflow issue	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10839
oss-security - Qemu: integer overflow issues	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20181008 Qemu: integer overflow issues
USN-3826-1: QEMU vulnerabilities | Ubuntu security notices	Patch Vendor Advisory usn.ubuntu.com text/html	UBUNTU USN-3826-1
1581013 – (CVE-2018-10839) CVE-2018-10839 Qemu: ne2000: integer overflow leads to buffer overflow issue	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1581013
Debian -- Security Information -- DSA-4338-1 qemu	Vendor Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4338
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:2892

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All

Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.10:*:*:*:*:*:*:*:

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

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

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

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report