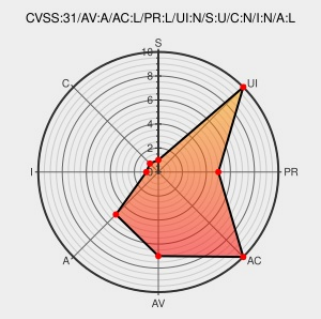
CVE-2015-6815

Published on: 01/31/2020 12:00:00 AM UTC

Last Modified on: 09/12/2023 02:55:00 PM UTC

CVE-2015-6815

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



Certain versions of Eos from Arista contain the following vulnerability:

The process_tx_desc function in hw/net/e1000.c in QEMU before 2.4.0.1 does not properly process transmit descriptor data when sending a network packet, which allows attackers to cause a denial of service (infinite loop and guest crash) via unspecified vectors.

CVE-2015-6815 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **QEMU** - **QEMU** version **= before 2.4.0.1**

CVSS3 Score: 3.5 - LOW

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

CVSS2 Score: 2.7 - LOW

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

CVE References

Description	Tags	Link
[Qemu-devel] [PATCH] e1000: Avoid infinite loop in processing transmit d	Mailing List Patch Third Party Advisory	CONFIRM lists.gnu.org/archive/html/qemu-devel/2015-09/msg01199.html

	Third Party Advisory lists.gnu.org text/x-diff	
oss-security - Re: CVE Request Qemu: net: e1000 infinite loop issue	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2015/09/05/5
Bug 1260076 – CVE-2015-6815 qemu: net: e1000: infinite loop issue	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1260076
[security-announce] SUSE-SU-2015:1894-1: important: Security update for	Mailing List Patch Third Party Advisory lists.opensuse.org text/html	MISC lists.opensuse.org/opensuse-security-announce/2015-11/msg00005.html
[security-announce] SUSE-SU-2015:1908-1: important: Security update for	Mailing List Patch Third Party Advisory lists.opensuse.org text/html	MISC lists.opensuse.org/opensuse-security-announce/2015-11/msg00011.html
[SECURITY] Fedora 21 Update: xen-4.4.3-4.fc21	Mailing List Third Party Advisory lists.fedoraproject.org text/html	MISC lists.fedoraproject.org/pipermail/package-announce/2015-October/168671.html
Arista - Security Advisory 0014	www.arista.com text/html	MISC www.arista.com/en/support/advisories-notices/security-advisories/1188-security-advisory-14
[SECURITY] Fedora 22 Update: xen-4.5.1-9.fc22	Mailing List Third Party Advisory lists.fedoraproject.org text/html	MISC lists.fedoraproject.org/pipermail/package-announce/2015-October/168646.html
[Qemu-devel] [ANNOUNCE] QEMU 2.4.0.1 CVE update released	Mailing List Patch Third Party Advisory lists.gnu.org text/html	CONFIRM lists.gnu.org/archive/html/qemu-devel/2015-09/msg05832.html
[security-announce] SUSE-SU-2015:1853-1: important: Security update for	Mailing List Patch Third Party Advisory lists.opensuse.org text/html	MISC lists.opensuse.org/opensuse-security-announce/2015-10/msg00026.html
oss-security - CVE Request Qemu: net: e1000 infinite loop issue	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2015/09/04/4
[SECURITY] Fedora 23 Update: xen-4.5.1-9.fc23	Mailing List Third Party Advisory lists.fedoraproject.org text/html	MISC lists.fedoraproject.org/pipermail/package-announce/2015-October/168077.html
USN-2745-1: QEMU vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	MISC www.ubuntu.com/usn/USN-2745-1

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Arista	Eos	4.12	All	All	All
Operating System	Arista	Eos	4.13	All	All	All
Operating System	Arista	Eos	4.14	All	All	All
Operating System	Arista	Eos	4.15	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Novell	Suse Linux Enterprise Debuginfo	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Debuginfo	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Debuginfo	11.0	sp3	All	All

Operating System	Novell	Suse Linux Enterprise Debuginfo	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp3	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp4	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating	Redhat	Enterprise Linux	5.0	All	All	All

System						
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Openstack	5.0	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	5.0	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Operating System	Xen	Xen	4.4.3	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.4.3	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All

cpe:2.3:o:arista:eos:4.12:*:*:*:*:*:*:*:

cpe:2.3:o:arista:eos:4.13:*:*:*:*:*:*:*:

cpe:2.3:o:arista:eos:4.14:*:*:*:*:*:*:*:

cpe:2.3:o:arista:eos:4.15:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

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

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

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

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:21:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:22:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:21:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:22:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_debuginfo:11.0:sp3:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_debuginfo:11.0:sp4:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_debuginfo:11.0:sp3:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_debuginfo:11.0:sp4:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_desktop:11.0:sp3:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_desktop:11.0:sp4:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_desktop:12.0:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_desktop:11.0:sp3:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_desktop:11.0:sp4:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_desktop:12.0:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_server:11.0:sp3:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_server:11.0:sp4:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_server:12.0:*:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_server:11.0:sp3:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_server:11.0:sp4:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_server:12.0:*:*:*:*:*:*:*:

cpe:2.3:a:novell:suse_linux_enterprise_software_development_kit:11.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:novell:suse_linux_enterprise_software_development_kit:11.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:novell:suse_linux_enterprise_software_development_kit:12.0:*:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_software_development_kit:11.0:sp3:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_software_development_kit:11.0:sp4:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_software_development_kit:12.0:*:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_software_development_kit:11.0:sp3:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_software_development_kit:11.0:sp4:*:*:*:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_software_development_kit:12.0:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→