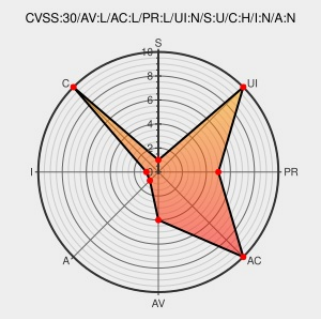
CVE-2018-1118

Published on: 05/10/2018 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:53:00 AM UTC

CVE-2018-1118

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



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

Linux kernel vhost since version 4.8 does not properly initialize memory in messages passed between virtual guests and the host operating system in the vhost/vhost.c:vhost_new_msg() function. This can allow local privileged users to read some kernel memory contents when reading from the /dev/vhost-net device file.

CVE-2018-1118 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **kernel** - **vhost** version **= since 4.8**

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
1573699 – (CVE-2018-1118) CVE-2018-1118 kernel: vhost:	Issue Tracking	CONFIRM

Information disclosure in vhost/vhost.c:vhost_new_msg()	Third Party Advisory bugzilla.redhat.com text/html	bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-1118
[SECURITY] [DLA 1423-1] linux-4.9 new package	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180718 [SECURITY] [DLA 1423-1] linux-4.9 new package
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:3083
CVE-2018-1118 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2018-1118
1573699 – (CVE-2018-1118) CVE-2018-1118 kernel: vhost: Information disclosure in vhost/vhost.c:vhost_new_msg()	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1573699
USN-3762-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3762-1
USN-3762-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3762-2
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:2948
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:3096

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	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	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	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

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:16.04:*:*:*:lts:*:*:*:

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

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

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

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization_host:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization_host:4.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→