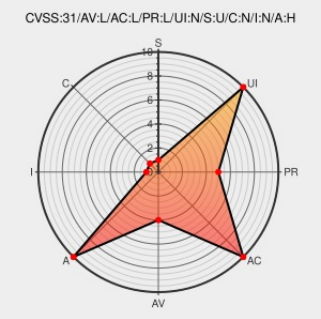
CVE-2018-15746

Published on: 08/29/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:27 PM UTC

CVE-2018-15746

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



Certain versions of Qemu from Qemu contain the following vulnerability:

qemu-seccomp.c in QEMU might allow local OS guest users to cause a denial of service (guest crash) by leveraging mishandling of the seccomp policy for threads other than the main thread.

CVE-2018-15746 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

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	NONE	NONE	HIGH

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
Red Hat Customer Portal	Third Party Advisory, access.redhat.com, text/html	REDHAT RHSA-2019:2425
oss-security - CVE-2018-15746 Qemu: seccomp:	Mailing List	MLIST [oss-security] 20180828 CVE-2018-15746 Qemu:

blacklist is not applied to all threads	Third Party Advisory www.openwall.com text/html	seccomp: blacklist is not applied to all threads
[Qemu-devel] [PATCH v4 4/4] seccomp: set the seccomp filter to all threa	Mailing List Patch Third Party Advisory lists.gnu.org text/x-diff	MLIST [qemu-devel] 20180822 [PATCH v4 4/4] seccomp: set the seccomp filter to all threads

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→