CVE-2018-20815

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-20815
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-31 22:29:00 UTC
Updated	2023-11-07 02:56:00 UTC
Description	In QEMU 3.1.0, load_device_tree in device_tree.c calls the deprecated load_image function, which has a buffer overflow ris

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	3.1.0	All	All	All
Application	Qemu	Qemu	3.1.0	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	
[SECURITY] Fedora 30 Update: qemu-3.1.0-9.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
[SECURITY] Fedora 29 Update: qemu-3.0.1-4.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Debian -- Security Information -- DSA-4506-1 qemu	DEBIAN	www.debian.org	
[SECURITY] Fedora 29 Update: qemu-3.0.1-4.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
git.qemu.org Git - qemu.git/commitdiff		git.qemu.org	
git.qemu.org Git - qemu.git/commitdiff	MISC	git.qemu.org	Mailin

Red Hat Customer Portal	REDHAT	access.redhat.com	
[SECURITY] Fedora 30 Update: qemu-3.1.0-9.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
Bugtraq: [SECURITY] [DSA 4506-1] qemu security update	BUGTRAQ	seclists.org	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710160 Gentoo Linux QEMU Multiple vulnerabilities (GLSA 201904-25)