



# CVE-2018-20815

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

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

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	3.1.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	3.1.0	All	All	All

## References

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

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

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)