



# CVE-2018-19873

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

## Summary

<b>CVE</b>	CVE-2018-19873
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-26 21:29:00 UTC
<b>Updated</b>	2020-09-28 09:15:00 UTC
<b>Description</b>	An issue was discovered in Qt before 5.11.3. QBmpHandler has a buffer overflow via BMP data.

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Application	<a href="#">Qt</a>	<a href="#">Qt</a>	All	All	All	All
Application	<a href="#">Qt</a>	<a href="#">Qt</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:1500-1: moderate: Security update f	SUSE	<a href="#">lists.opensuse.org</a>	
[security-announce] openSUSE-SU-2020:1501-1: moderate: Security update f	SUSE	<a href="#">lists.opensuse.org</a>	
[SECURITY] [DLA 1786-1] qt4-x11 security update	MLIST	<a href="#">lists.debian.org</a>	
[SECURITY] [DLA 2377-1] qt4-x11 security update	MLIST	<a href="#">lists.debian.org</a>	
[security-announce] openSUSE-SU-2018:4261-1: moderate: Security update f	SUSE	<a href="#">lists.opensuse.org</a>	Mailing List, Third P
Qt 5.11.3 Released with Important Security Updates	CONFIRM	<a href="#">blog.qt.io</a>	Release Notes, Ver
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	

Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
Debian -- Security Information -- DSA-4374-1 qtbase-opensource-src	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Third Party Advisory
USN-4003-1: Qt vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
[security-announce] openSUSE-SU-2020:1530-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
Gerrit Code Review	CONFIRM	<a href="https://codereview.qt-project.org">codereview.qt-project.org</a>	Issue Tracking, Pat
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
[SECURITY] [DLA 1627-1] qtbase-opensource-src security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing List, Third P
[security-announce] openSUSE-SU-2020:1452-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[377444](#) Alibaba Cloud Linux Security Update for qt (ALINUX2-SA-2020:0049)

[377505](#) Alibaba Cloud Linux Security Update for qt5 (ALINUX2-SA-2019:0095)

© [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)