



CVE-2018-19665

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

Summary

| | |
|------------------------|----------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2018-19665 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-12-06 23:29:00 UTC |
| Updated | 2020-12-14 20:19:00 UTC |
| Description | The Bluetooth subsystem in QEMU mishandles negative values for length variables, leading to memory corruption. |

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------------------------|----------------------|---------|--------|---------|----------|
| Operating System | Opensuse | Leap | 42.3 | All | All | All |
| Operating System | Opensuse | Leap | 42.3 | All | All | All |
| Application | Qemu | Qemu | 3.1.0 | rc0 | All | All |
| Application | Qemu | Qemu | 3.1.0 | rc0 | All | All |
| Application | Qemu | Qemu | All | All | All | All |

References

| Reference | Source | Link |
|---------------------------------------------------------------------------------------------------------|---------|------------------------------------------------------------------|
| oss-security - CVE-2018-19665 Qemu: bt: integer overflow in Bluetooth routines allows memory corruption | MLIST | www.openwall.com |
| [security-announce] openSUSE-SU-2019:1226-1: important: Security update | SUSE | lists.opensuse.org |
| [Qemu-devel] [PATCH v2] bt: use size_t type for length parameters instea | MLIST | lists.gnu.org |
| QEMU CVE-2018-19665 Integer Overflow Vulnerability | BID | www.securityfocus.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy OID Mappings

900187 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

903269 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1963)

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)