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.
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

Legacy QID 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)