# CVE-2020-12829

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-12829 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-08-31 15:15:00 UTC |
| **Updated** | 2020-12-14 20:22:00 UTC |
| **Description** | In QEMU through 5.0.0, an integer overflow was found in the SM501 display driver implementation. This flaw occurs in the |

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 20.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 20.04 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |

## References

| Reference |
|---|
| 1808510 – (CVE-2020-12829) CVE-2020-12829 qemu: OOB read and write due to integer overflow in sm501_2d_operation() in hw/display/sm |
| Debian -- Security Information -- DSA-4760-1 qemu |
| USN-4467-1: QEMU vulnerabilities \| Ubuntu security notices \| Ubuntu |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- 174920 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1243-1)
- 174921 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1245-1)
- 174922 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1240-1)
- 174923 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1241-1)
- 174924 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1244-1)
- 174926 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1242-1)
- 750251 OpenSUSE Security Update for qemu (openSUSE-SU-2021:0600-1)
- 900187 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
- 903467 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (2183)
- 905852 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (2183-1)