



# CVE-2018-5748

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

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2018-5748                                                                                                            |
| <b>State</b>           | PUBLIC                                                                                                                   |
| <b>Assigner</b>        | cve@mitre.org                                                                                                            |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2018-01-25 16:29:00 UTC                                                                                                  |
| <b>Updated</b>         | 2020-10-15 13:28:00 UTC                                                                                                  |
| <b>Description</b>     | qemu/qemu_monitor.c in libvirt allows attackers to cause a denial of service (memory consumption) via a large QEMU reply |

## Risk And Classification

**Problem Types:** CWE-400

## 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>                | 7.0     | 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="#">Debian</a> | <a href="#">Debian Linux</a>                | 7.0     | 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="#">Redhat</a> | <a href="#">Enterprise Linux Desktop</a>    | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Desktop</a>    | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Desktop</a>    | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Desktop</a>    | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>     | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>     | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>     | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>     | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a> | 7.6     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a> | 7.6     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a> | 7.5     | All    | All     | All      |

|                  |                        |                                              |     |     |     |     |
|------------------|------------------------|----------------------------------------------|-----|-----|-----|-----|
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a>  | 7.6 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a>  | 7.5 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a>  | 7.6 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Tus</a>  | 7.6 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Tus</a>  | 7.6 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 7.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 7.0 | All | All | All |
| Application      | <a href="#">Redhat</a> | <a href="#">Libvirt</a>                      | -   | All | All | All |
| Application      | <a href="#">Redhat</a> | <a href="#">Libvirt</a>                      | -   | All | All | All |

| References                                                               |         |                                       |                             |
|--------------------------------------------------------------------------|---------|---------------------------------------|-----------------------------|
| Reference                                                                | Source  | Link                                  | Tags                        |
| [libvirt] [PATCH] qemu: avoid denial of service reading from QEMU monito | MLIST   | <a href="#">www.redhat.com</a>        | Patch, Third Party Adviso   |
| Red Hat Customer Portal                                                  | REDHAT  | <a href="#">access.redhat.com</a>     | Third Party Advisory        |
| [SECURITY] [DLA 1315-1] libvirt security update                          | MLIST   | <a href="#">lists.debian.org</a>      | Mailing List, Third Party A |
| Red Hat Customer Portal                                                  | REDHAT  | <a href="#">access.redhat.com</a>     | Third Party Advisory        |
| libvirt 'qemu/qemu_monitor.c' Local Denial of Service Vulnerability      | BID     | <a href="#">www.securityfocus.com</a> | Third Party Advisory, VDE   |
| Debian -- Security Information -- DSA-4137-1 libvirt                     | DEBIAN  | <a href="#">www.debian.org</a>        | Third Party Advisory        |
| CVE Program record                                                       | CVE.ORG | <a href="#">www.cve.org</a>           | canonical                   |
| NVD vulnerability detail                                                 | NVD     | <a href="#">nvd.nist.gov</a>          | canonical, analysis         |

No vendor comments have been submitted for this CVE.

| Legacy QID Mappings                                                                   |
|---------------------------------------------------------------------------------------|
| <a href="#">710202</a> Gentoo Linux libvirt Multiple Vulnerabilities (GLSA 201804-07) |