



# CVE-2019-18806

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

## Summary

|                        |                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2019-18806                                                                                                                 |
| <b>State</b>           | PUBLIC                                                                                                                         |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                   |
| <b>Published</b>       | 2019-11-07 16:15:00 UTC                                                                                                        |
| <b>Updated</b>         | 2020-08-24 17:37:00 UTC                                                                                                        |
| <b>Description</b>     | A memory leak in the ql_alloc_large_buffers() function in drivers/net/ethernet/qlogic/qla3xxx.c in the Linux kernel before 5.3 |

## Risk And Classification

**Problem Types:** CWE-401

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                | Product                      | Version | Update | Edition | Language |
|------------------|-----------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | All     | All    | All     | All      |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | All     | All    | All     | All      |

## References

| Reference                                                                                                                       | Source  | Link                                                | Tags                                      |
|---------------------------------------------------------------------------------------------------------------------------------|---------|-----------------------------------------------------|-------------------------------------------|
| <a href="https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.5">cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.5</a> | MISC    | <a href="https://cdn.kernel.org">cdn.kernel.org</a> | Mailing List, Vendor Advisory             |
| <a href="https://kernel/git/torvalds/linux.git">kernel/git/torvalds/linux.git</a> - Linux kernel source tree                    | MISC    | <a href="https://git.kernel.org">git.kernel.org</a> | Mailing List, Patch, Third Party Advisory |
| 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.

There are currently no legacy QID mappings associated with this CVE.

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)