

## Overall Rating - High



This notification is intended as an informational bulletin for technical audiences.

### Summary

The Vulnerability and Risk Management (VRM) Team is aware of a use-after-free vulnerability in Netfilter nf\_tables in the Linux kernel through 6.3.1.

### Technical Details

When processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled.

This vulnerability is rated as a **High** Severity.

### Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify [VRM](#) with any questions or concerns you may have.

### References

- [CVE-2023-32233](#)
- <http://packetstormsecurity.com/files/173087/Kernel-Live-Patch-Security-Notice-LSN-0095-1.html>
- <http://www.openwall.com/lists/oss-security/2023/05/15/5>
- [https://bugzilla.redhat.com/show\\_bug.cgi?id=2196105](https://bugzilla.redhat.com/show_bug.cgi?id=2196105)
- <https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c1592a89942e9678f7d9c8030efa777c0d57edab>
- <https://github.com/torvalds/linux/commit/c1592a89942e9678f7d9c8030efa777c0d57edab>
- <https://lists.debian.org/debian-lts-announce/2023/06/msg00008.html>
- <https://lists.debian.org/debian-lts-announce/2023/07/msg00030.html>
- <https://news.ycombinator.com/item?id=35879660>
- <https://security.netapp.com/advisory/ntap-20230616-0002/>
- <https://www.debian.org/security/2023/dsa-5402>
- <https://www.openwall.com/lists/oss-security/2023/05/08/4>