November 8, 2023

Overall rating: Critical

BRITISH COLUMBIA

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware Red Hat has published a Security. Bulletin to address Multiple products. Included were critical updates for the following:

- Redis RedisGraph – version v.2.x to v.2.12.8

Technical Details

Squid is vulnerable to a Denial of Service, where a remote attacker can perform buffer overflow attack by writing up to 2 MB of arbitrary data to heap memory when Squid is configured to accept HTTP Digest Authentication.

This vulnerability is rated as a **Critical** 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-2023-47004, CVE-2023-46847
- Red Hat Security Advisory – CVE-2023-47004
- Red Hat Security Advisories

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts