Overall rating: High

BRITISH COLUMBIA

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware of multiple recently disclosed Apache Traffic Server vulnerabilities.

Technical Details

- **Improper Input Validation vulnerability.**
  The configuration option proxy.config.http.push_method_enabled didn't function. However, by default the PUSH method is blocked in the ip_allow configuration file.This issue affects Apache Traffic Server: from 8.0.0 through 9.2.0. 8.x users should upgrade to 8.1.7 or later versions 9.x users should upgrade to 9.2.1 or later versions. CVE-2023-30631

- **Exposure of Sensitive Information to an Unauthorized Actor vulnerability**
  This issue affects Apache Traffic Server: from 8.0.0 through 9.2.0. 8.x users should upgrade to 8.1.7 or later versions 9.x users should upgrade to 9.2.1 or later versions. CVE-2023-33933.

- **Exposure of Sensitive Information to an Unauthorized Actor vulnerability**.
  This issue affects Apache Traffic Server: 8.0.0 to 9.2.0. CVE-2022-47184

These vulnerabilities are rated as an overall **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-2023-30631, CVE-2023-33933, CVE-2022-47184
- https://lists.apache.org/thread/tns2b4khyyncgs5v5p9y35pobg9z2bvs
- https://www.debian.org/security/2023/dsa-5435
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/6GDCBNFDDW6ULW7CACJCPENI7BVDHM5O/
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/FGWXNAEEVRUZ5JG4EJAIIFC3CI7LFETV/
- https://lists.debian.org/debian-lts-announce/2023/06/msg00037.html