July 11, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Apache HTTP Server vulnerability. The vulnerability affects Apache HTTP Server versions prior to 2.1.61.

Technical Details

A regression in the core of Apache HTTP Server 2.4.60 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have atVulnerabilityandRiskManagement@gov.bc.ca.

References

- Apache HTTP Server 2.4
- CVE-2024-39884
- Tenable CVE-2024-39884
- VRM Vulnerability Reports