August 9, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of ah Apache http server vulnerability. The vulnerability affects Apache http server versions prior to 2.4.62.

Technical Details

A partial fix for CVE-2024-39884 in the core of Apache HTTP Server 2.4.61 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.

Additionally, SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests.

Users are recommended to upgrade to version 2.4.62 which fixes this issue.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **HIGH** 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

- CVE-2024-40725, CVE-2024-40898
- Apache HTTP Server 2.4 vulnerabilities
- Apache 2.4.x < 2.4.62 Multiple Vulnerabilities
- VRM Vulnerability Reports