August 9, 2024

Overall Rating: Medium

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a F5 vulnerability. The vulnerability affects the Apache HTTPD component in BIG-IP versions 15.1.0 - 15.1.10, 16.1.0 - 16.1.5, 17.1.0 - 17.1.1.

Technical Details

Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure. Substitutions in server context that use a backreferences or variables as the first segment of the substitution are affected. Some unsafe RewiteRules will be broken by this change and the rewrite flag "UnsafePrefixStat" can be used to opt back in once ensuring the substitution is appropriately constrained.

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

This vulnerability is rated as a **MEDIUM** 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-2024-38474, CVE-2024-38475
- K000140620: Apache HTTPD vulnerabilities CVE-2024-38474 and CVE-2024-38475
- VRM Vulnerability Reports