April 12, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Apache published a security advisory to address a vulnerability in the following products:

- Apache HTTP Server: through 2.4.58

Technical Details
Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses.
This issue affects Apache HTTP Server: through 2.4.58.

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

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

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.

References

- CVE-2024-27316 CVE-2023-38709 CVE-2024-24795
- Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project