مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Apache

Tracking #:432316013

Date:03-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Apache released security updates to address several vulnerabilities in their products.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-36387** | Apache HTTP Server: DoS by Null pointer in websocket over HTTP/2
  - Serving WebSocket protocol upgrades over a HTTP/2 connection could result in a Null Pointer dereference, leading to a crash of the server process, degrading performance.
- **CVE-2024-38472** | Apache HTTP Server on WIndows UNC SSRF
  - SSRF in Apache HTTP Server on Windows allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests or content
- **CVE-2024-38473** | Apache HTTP Server proxy encoding problem
  - Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests.
- **CVE-2024-38474** | Apache HTTP Server weakness with encoded question marks in backreferences
  - 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.
- **CVE-2024-38475** | Apache HTTP Server weakness in mod_rewrite when first segment of substitution matches filesystem path
  - 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.
- **CVE-2024-38476** | Apache HTTP Server may use exploitable/malicious backend application output to run local handlers via internal redirect
  - Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable.

- **CVE-2024-38477** | Apache HTTP Server: Crash resulting in Denial of Service in mod_proxy via a malicious request
    - null pointer dereferences in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.
- **CVE-2024-39573** | Apache HTTP Server: mod_rewrite proxy handler substitution
    - Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy.

Affected Versions:

- Apache HTTP Server versions <=2.4.59

Fixed Versions:

- Apache HTTP Server version 2.4.60

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Apache.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://httpd.apache.org/security/vulnerabilities_24.html