مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Apache HTTP Server

Tracking #:432318899

Date:05-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in the Apache HTTP Server Project that could allow attackers to execute arbitrary code, bypass authentication, escalate privileges, or disrupt service availability.

TECHNICAL DETAILS:

Vulnerability Details

CVE-2026-23918

- **Severity:** Important
- Double free vulnerability in HTTP/2 triggered by early connection reset conditions.

CVE-2026-33006

- **Severity:** Moderate
- Timing attack in mod_auth_digest allowing authentication bypass.

CVE-2026-24072

- **Severity:** Moderate
- Improper access control in .htaccess processing allows privilege escalation to httpd user level.

CVE-2026-34059, CVE-2026-34032, CVE-2026-33857

- **Severity:** Low
- Memory corruption issues in mod_proxy_ajp leading to potential information disclosure.

CVE-2026-33007

- **Severity:** Low
- NULL pointer dereference in mod_authn_socache causing denial of service.

CVE-2026-29169

- **Severity:** Low
- NULL pointer dereference in mod_dav_lock resulting in service crash.

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code on the server, bypass authentication mechanisms, escalate privileges, or cause denial of service conditions, potentially resulting in full system compromise and service disruption.

Affected Versions

- Apache HTTP Server versions 2.4.0 through 2.4.66

Fixed Versions

- Apache HTTP Server 2.4.67 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Apache HTTP Server Project.

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/download.cgi#apache24
- https://httpd.apache.org/security/vulnerabilities_24.html