مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Apache HTTP Server

Tracking #:432319121

Date:13-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Apache HTTP Server. These vulnerabilities could allow attackers to cause denial of service, memory corruption, buffer overflows, cross-site scripting (XSS), privilege escalation, and unauthorized file access under certain conditions.

TECHNICAL DETAILS:

Vulnerability Details
Moderate Severity:

- **CVE-2026-34355**
  A buffer overflow vulnerability in mod_proxy_html that can be triggered by a malicious or untrusted backend server.
- **CVE-2026-42535**
  A path handling flaw in mod_dav_fs that may allow manipulation of DAV property databases and cause child process crashes.
- **CVE-2026-43951**
  An out-of-bounds read vulnerability in merge_response_headers that may result in service crashes.
- **CVE-2026-44119**
  An improper privilege management vulnerability that allows local .htaccess authors to read files with the privileges of the Apache HTTP Server process.
- **CVE-2026-44186**
  An infinite loop condition in mod_proxy_ftp that could lead to denial of service when communicating with malicious FTP backends.
- **CVE-2026-49975**
  A denial-of-service vulnerability in mod_http2 caused by excessive memory allocation through malicious HTTP requests.

Low Severity:

- **CVE-2026-29167**
  A use-after-free vulnerability in mod_ldap per-directory configuration that could lead to memory corruption.
- **CVE-2026-29170**
  A cross-site scripting (XSS) vulnerability in mod_proxy_ftp when generating HTML directory listings for FTP content.
- **CVE-2026-34356**
  A heap-based buffer overflow in ProxyPassReverseCookie* processing when interacting with malicious backend servers.
- **CVE-2026-42536**
  A heap-based buffer overflow in mod_xml2enc when processing untrusted content.
- **CVE-2026-44185**
  A stack buffer over-read vulnerability in mod_ssl during outbound OCSP requests to attacker-controlled OCSP servers.
- **CVE-2026-44631**
  A heap underflow vulnerability in ap_regname triggered through crafted regular expressions in configuration files.
- **CVE-2026-48913**
  A use-after-free vulnerability in mod_http2 that may occur when file handles are exhausted.

Affected Versions

- Apache HTTP Server 2.4.67 and earlier

Fixed Version:

- Apache HTTP Server 2.4.68 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions 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