مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Request Smuggling Vulnerability in Apache Traffic Server

Tracking #:432317038

Date:04-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a request smuggling vulnerability (CVE-2024-53868) has been identified in Apache Traffic Server (ATS), a high-performance HTTP proxy server widely used by content delivery networks (CDNs) and major content owners.

TECHNICAL DETAILS:

A request smuggling vulnerability (CVE-2024-53868) has been identified in Apache Traffic Server (ATS), a high-performance HTTP proxy server widely used by content delivery networks (CDNs) and major content owners.

Vulnerability Details:

- CVE ID: CVE-2024-53868
- Severity: High
- Type: Request Smuggling via Chunked Transfer Encoding
- Successful exploitation could lead to:
  - Security Control Bypass: Evade web application firewalls (WAFs) or access restrictions.
  - Cache Poisoning: Serve malicious content to legitimate users via cached responses.
  - Session Hijacking: Intercept or manipulate user sessions through smuggled requests.
- Affected Versions
  - 9.x series: 9.0.0 through 9.2.9
  - 10.x series: 10.0.0 through 10.0.4
- Fixed Versions
  - 9.x: Patch available in 9.2.10
  - 10.x: Patch available in 10.0.5

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade Apache Traffic Server to the fixed versions as soon as possible.

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://lists.apache.org/thread/rwyx91rsrnmpjbm04footfjjf6m9d1c9