مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Apache Traffic Server

Tracking #:432316952

Date:10-03-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Apache Traffic Server project has released security updates to address multiple vulnerabilities affecting various versions of its web proxy cache. These vulnerabilities pose significant risks, including request smuggling, improper access control, and potential denial-of-service conditions.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-38311: Request Smuggling via Pipelining after Chunked Message Body**
  - This vulnerability stems from improper input validation, allowing attackers to perform request smuggling through pipelining after a chunked message body.
  - Impact: Attackers can manipulate network traffic and potentially gain unauthorized access to sensitive information.
- **CVE-2024-56195: Improper Access Control in Intercept Plugins**
  - Intercept plugins lack proper access controls, enabling unauthorized modification of network traffic.
  - Impact: Attackers can potentially intercept and modify network traffic, leading to data breaches or other malicious activities.
- **CVE-2024-56196: Improper Access Control in Access Control Lists (ACLs)**
  - This vulnerability affects compatibility with older versions of Apache Traffic Server and relates to improper ACL implementation.
  - Impact: Attackers could bypass access control restrictions.
- **CVE-2024-56202: Expect Header Field Expected Behavior Violation**
  - This vulnerability allows attackers to "unreasonably retain resources" by exploiting the Expect header field.
  - Impact: Potential for denial-of-service (DoS) attacks.

Affected Versions:

- Apache Traffic Server 9.0.0 to 9.2.8 (CVE-2024-38311, CVE-2024-56195, CVE-2024-56202)
- Apache Traffic Server 10.0.0 to 10.0.3 (CVE-2024-38311, CVE-2024-56195, CVE-2024-56196, CVE-2024-56202)

Fixed Versions:

- Apache Traffic Server version **9.2.9** or **10.0.4**

RECOMMENDATIONS:

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

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/btofzws2yqskk2n7f01r3l1819x01023