مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Security Vulnerabilities in Apache Traffic Server

Tracking #:432316519

Date:18-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed The Apache Software Foundation has recently released a security update for Apache Traffic Server (ATS), addressing multiple vulnerabilities including a critical one.

TECHNICAL DETAILS:

The Apache Software Foundation has recently released a security update for Apache Traffic Server (ATS), addressing multiple vulnerabilities including a critical one with severe implications for affected systems. The flaws expose ATS to attacks that could result in cache poisoning, denial-of-service (DoS) disruptions, and privilege escalation, potentially granting attackers full control over impacted servers.

Vulnerabilities Details:

1. **CVE-2024-50306: Privilege Escalation on Startup (CVSS 9.1)-**This critical vulnerability occurs due to an unchecked return value during startup, allowing Apache Traffic Server to retain elevated privileges. This could lead to privilege escalation, where attackers could gain unauthorized access to the server with root or administrative-level privileges.
2. **CVE-2024-38479: Cache Key Plugin Vulnerability (CVSS 7.5)-**The vulnerability arises in the cache key plugin of Apache Traffic Server, which can be manipulated by attackers to inject malicious content into the server's cache. This could result in cache poisoning, where users may be redirected to malicious websites or served malicious content, including malware.
3. **CVE-2024-50305: Host Field Vulnerability (CVSS 7.5)-**A specially crafted **Host** field in HTTP requests can trigger a crash in Apache Traffic Server, leading to a denial-of-service (DoS) condition. Attackers can exploit this flaw to disrupt server operations, causing web services to become unavailable and impacting the availability of websites relying on ATS.

Version Affected:

- ATS 9.0.0 to 9.2.5 (CVE-2024-38479, CVE-2024-50305, CVE-2024-50306)
- ATS 10.0.0 to 10.0.1 (CVE-2024-50306)

Mitigation:

- 9.x users should upgrade to 9.2.6 or later versions
- 10.x users should upgrade to 10.0.2 or later versions

RECOMMENDATIONS:

- Ensure that the latest patches are applied as soon as possible to reduce the risk of exploitation.
- Monitor for unusual activity: Implement logging and monitoring solutions to detect any suspicious behavior or attempted exploitation of the vulnerabilities.

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/y15fh6c7kyqvzm0f9odw7c5jh4r4np0y