NATIONAL CSIRT-CY

CVE-2025-49763

20/06/2025

Apache Traffic Server vulnerability allows DOS attack.

CONFIDENTIAL

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

Executive Summary

Security researchers discovered that a critical vulnerability exists in Apache Traffic Server. It allows attackers to remotely cause denial-of-service (DoS) attacks via memory resource exhaustion.

This vulnerability affects the Edge Side Includes (ESI) plugin.

This specific attack can be executed remotely without requiring authentication or privileged access.

This vulnerability is having a high CVSS score of 7.5

Users should apply the latest updates to the following versions:

- Apache Traffic Server 9.x: Patched in 9.2.11 and later versions.
- Apache Traffic Server 10.x: Patched in 10.0.6 and later versions.

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-49763

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/400.html

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.