Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 148 **12-01-2022**

Name: Apache Traffic Server vulnerable to Cache Poisoning attack for CDNs (CVE-2021-27577)

Threat Classification: Cache Poisoning

Affected Versions:

- Apache Traffic Server 7.0.0 to 7.1.12
- Apache Traffic Server 8.0.0 to 8.1.1
- Apache Traffic Server 9.0.0 to 9.0.1

Summary:

Recently, more than 70 flaws discovered in combinations of cloud applications and content delivery networks (CDNs) that could be used to poison the CDN caches and result in denial-of-service (DoS) attacks on the applications. The vulnerability exists due to insufficient validation of user-supplied input when handling URL fragmentation. A remote attacker can send specially crafted HTTP request and poison the web server cache.

Severity	**High**
Attack Vector	**Network**
Privileges required	**None**

For further details, please visit following official link:
https://lists.apache.org/thread/c6qkdb4srn6xksgmztw82p6srmo2kmq1

Recommendations:

- Please visit the website link and follow **mitigations** for the aforementioned vulnerability:

  https://lists.apache.org/thread/c6qkdb4srn6xksgmztw82p6srmo2kmq1

  https://trafficserver.apache.org/downloads

- It is recommended to install updates from vendor's website at earliest.
- Users should upgrade to **8.1.2** or **9.0.2**, or later versions.
- Always use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Designate a PoC from your security / Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office or PTA CERT portal.