Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 147 **10-01-2022**

Name: Cache Poisoning vulnerabilities in web server cache **(**CVE-2021-27577**)**

Threat Classification: Remote Code Execution

Affected Versions:

Apache Traffic Server 7.0.0 to 7.1.12

ATS 8.0.0 to 8.1.1

ATS 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. A single request, when cached, can cause a site, service, or specific page to become inaccessible for hours, depending on the length of time between cache refreshes. Any Web or API request that a CDN passes to the application that causes the application to throw an exception could poison the cache.

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

For further details, please visit following link:
https://www.cvedetails.com/cve/CVE-2021-27577/

© Copyright 2021, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.

Recommendations:

- Please visit the website link and check **mitigations** for the aforementioned vulnerabilities:
  https://lists.apache.org/thread/c6qkdb4srn6xksgmztw82p6srmo2kmq1
  https://trafficserver.apache.org/downloads

- It is recommended to install updates from vendor's website.
- Users should upgrade to **8.1.2** or **9.0.2**, or later versions.
- Don't accept fat ***GET*** requests. Be aware that some third-party technologies may permit this by default.
- 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.

© Copyright 2021, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.