# Pakistan Telecom Authority, Islamabad

## PTA Cyber Security Advisory No: 090

09-July-2020

**Name:** f5 BIG-IP Critical Remote Code Execution (RCE) Vulnerability (CVE-2020-5902)

**Affected Systems:** Affects the following BIG-IP versions:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM)

**Summary:**

The Traffic Management User Interface (TMUI)/ Configuration utility, has a remote code execution (RCE) vulnerability which could allow an attacker, with network access to the Configuration utility or TMUI, to execute arbitrary commands. This may result in a complete system compromise.

| Severity | CRITICAL |
|---|---|
| Attack Vector | Network |
| Attack Complexity | Low |
| Privileges required | None |

The BIG-IP system in Appliance mode is also vulnerable. For further details, please visit following official link:
https://support.f5.com/csp/article/K52145254

**Recommendations:**

- Please visit following official link for the mitigation of the aforementioned vulnerability: https://support.f5.com/csp/article/K52145254
- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.
- In all cases, also ensure that devices to be upgraded to new release meet the requirements set by the vendor.
- Whenever required, access the system with minimal access rights and privileges.
- 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.