Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 150 **10-05-2022**

Name: F5 BIG-IP iControl REST Vulnerability

(CVE-2022-1388)

Threat Classification: Remote Code Execution

Affected Versions:

- 1.0 to 16.1.2
- 1.0 to 15.1.5
- 1.0 to 14.1.4
- 1.0 to 13.1.4
- 1.0 to 12.1.6
- 6.1 to 11.6.5

Summary:

CVE-2022-1388 is a critical vulnerability (CVSS 9.8) in the management interface of F5 Networks' BIG-IP solution that enables an unauthenticated attacker to gain remote code execution on the system through bypassing F5's iControl REST authentication. The vulnerability was first discovered by F5's internal product security team and disclosed publicly on May 4, 2022.

Through a combination of software and hardware, F5 BIG-IP allows the inspection and encryption of traffic passing through a network. It serves as a load balancer, application firewall, and full proxy. F5 BIG-IP is widely adopted and is one of the most commonly exposed services seen across Randori customer attack surfaces. According to F5, BIG-IP is used by 48 of the Fortune 50 and there are more than 16,000 instances of BIG-IP discoverable by Shodan; however, the management interface needed to exploit this vulnerability is rarely internet-facing or publicly exposed.

Severity	Critical
CVS Score	9.8
Attack Vector	Network
Privileges required	None

Recommendations:

- Please visit the website link and check **mitigations** and **workarounds** for the aforementioned vulnerabilities:
  https://support.f5.com/csp/article/K23605346
- It is recommended to **update** the version from vendor website.
- Block iControl REST access through the self IP address
- Block iControl REST access through the management interface
- Modify the BIG-IP https configuration
- 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.