Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 140 **23-08-2021**

Name: Critical FortiWeb (WAF) SQL Injection Vulnerability

Threat Classification: Command Injection

Affected Products:

- FortiWeb versions 6.3.7 and below
- FortiWeb versions 6.2.3 and below

Summary:

A command injection vulnerability (CVE-2020-29015) has been reported to be found in Fortinet FortiWeb (WAF), and the security report claimed that Fortinet will soon release a fix for this vulnerability. A blind SQL injection in the user interface of FortiWeb may allow an unauthenticated, remote attacker to execute arbitrary SQL queries or commands by sending a request with a crafted Authorization header containing a malicious SQL statement.

Severity	Critical
Attack Vector	Network
Privileges required	None

For further details, please visit following official link:

- https://www.fortiguard.com/psirt/FG-IR-20-124

Recommendations:

- Please upgrade/ patch FortiWeb versions series 6.2.X and 6.3.X as per the vendor recommendations:
  - Please upgrade to **FortiWeb versions 6.3.8 or above**
  - Please upgrade to **FortiWeb versions 6.2.4 or above**
- FortiWeb device's management interface from suspicious networks including internet must be blocked.
- It is also recommended to access FortiWeb management interface through trusted networks only and using secure VPN.
- 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.