Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No: 61 **05-December-2019**

Threat Classification: Cross-site Scripting (XSS) and Path traversal Vulnerabilities

Name: Fortinet FortiOS SSL VPN XSS and Path traversal vulnerabilities

Affected Systems: Affects the following products of Fortinet:

XSS Vulnerability

- FortiOS 6.0.0 to 6.0.4
- FortiOS 5.6.0 to 5.6.7
- FortiOS 5.4.0 to 5.4.12
- FortiOS 5.2 branch and below

Path traversal Vulnerability

- FortiOS 6.0.0 to 6.0.4
- FortiOS 5.6.3 to 5.6.7
- FortiOS 5.4.6 to 5.4.12

Resolved versions:

- **FortiOS 5.4.13, 5.6.8, 6.0.5 or 6.2.0 and above**

Summary:

An attacker may perform a Cross-site Scripting (XSS) attack due to error/message handling parameter sanitization failure in the web portal of FortiOS SSL VPN. Also, a vulnerability in the same web portal may allow an attacker to download the system files of FortiOS through specially crafted HTTP requests resulting in sensitive information disclosure.

Attack Severity	High
Attack Vector	Network
Attack Type	XSS and Path traversal

Recommendations:

- For official recommended upgrade path, visit following website link to fix the aforementioned vulnerabilities:
  https://docs.fortinet.com/upgrade-tool

- Mitigating the impact of the said exploit may also be done by enabling two-factor authentication for SSL VPN users.

- In all cases, ensure the availability of stable version by the relevant vendor, before upgrade.

- 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.