Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 141 **14-09-2021**

Name: Leaked FortiGate SSL-VPN Credentials (CVE-2018-13379)

Threat Classification: Path Traversal Vulnerability

Affected Products:

FortiOS 6.0 – 6.0.0 to 6.0.4

FortiOS 5.6 – 5.6.3 to 5.6.7

FortiOS 5.4 – 5.4.6 to 5.4.12

Summary:

Fortinet has notified that a cybercriminal gang has assembled a collection of access credentials for thousands of FortiGate SSL-VPN devices. Credentials were stolen from systems that **remain unpatched against a two-year-old vulnerability CVE-2018-13379** or from users who patched that vulnerability but **failed** to change passwords. The vulnerability in FortiOS SSL VPN web portal may allow an attacker to download FortiOS system files through specially crafted HTTP resource requests.

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

For further details, please visit following vendor link:
https://www.fortinet.com/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials

Recommendations:

- Please visit the website link and check remediation and workarounds for the aforementioned vulnerability:
  https://www.fortinet.com/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials

- Disable all VPNs (SSL-VPN or IPSEC) until the necessary remediation steps have been taken.
- It is recommended to **upgrade** to FortiOS 5.4.13, 5.6.8, 6.0.5 or 6.2.0 and above as per the product version.
- Treat all credentials as potentially compromised and perform an organization-wide password reset.
- Implement multi-factor authentication (MFA), which would help mitigate the abuse of any compromised credentials.
- 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.
- In case of any incident, please report to this office.