PTA Security Advisory-No: 41

12-March-2019

Threat Classification: Security Vulnerability

Name: Information Disclosure Vulnerability (CVE-2016-2183)

Overview: Several vulnerabilities have been discovered in Fortinet products, a remote attacker could exploit these vulnerabilities to trigger Remote Code Execution and reveal the sensitive Information on the targeted system.

Source: Affected following products of Fortinet products:

- FortiOS
- FortiAnalyzer
- FortiManager
- FortiOS Web adminUI
- FortiOS SSL VPN Web Portal
- FortiOS VIP, WANOpt, VoIP
- FortiOS webfilter override and authentication service
- FortiAP
- FortiSwitch

Distribution: The vulnerabilities can be exploited in the following versions of Fortinet:

- FortiOS Web adminUI: 5.0.5 and below
- FortiOS SSL VPN Web Portal: 5.2.9 and below, 5.4.0, 5.4.1
- FortiOS VIP, WANOpt, VoIP: 5.4.4 and below
- FortiOS webfilter override and authentication service: 5.4.8 and below, 5.6.0 to 5.6.3
- FortiAP 5.4.4 and below, 5.6.0 to 5.6.4, 6.0.0
- FortiAnalyzer 5.2.9 and below, 5.4.0, 5.4.1, 5.4.6 and above for 5.4 branch,6.0.2
- FortiSwitch 3.6.7 and below, 6.0.0, 6.0.1

Exploited Vulnerabilities: Hackers can exploit above vulnerabilities exist in the multiple products of Fortinet, The remote attackers can obtain plaintext data from long connected encrypted session through birthday attack, in order to gain access on sensitive information of the targeted system.

Recommendations:

- Use the following official patches/commands to fix the aforementioned vulnerabilities:
  - https://fortiguard.com/psirt/FG-IR-17-173
- Whenever possible, run software 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 avoids download/use of crack and pirated software.
- Designate a PoC for your network users for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.