PTA Security Advisory-No: 44

25-March-2019

Threat Classification: Security Vulnerability

Name: Remote Command Execution Vulnerability (CVE-2019-1663)

Source: Affect following products of Cisco:

- Cisco Wireless-N VPN Firewall
- Cisco Wireless-N VPN Router
- Cisco Wireless-N Multifunction VPN Router

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

- Cisco RV110W Wireless-N VPN Firewall 1.2.2.1 and prior versions
- Cisco RV215W Wireless-N VPN Router 1.3.1.1 and prior versions
- Cisco RV130W Wireless-N Multifunction VPN Router 1.0.3.45 and prior versions

Exploited Vulnerabilities: The vulnerability is due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit this vulnerability by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the base operating system of an affected device as a high-privilege user.

Recommendations:

- Update firmware of respective device from following official website to fix the aforementioned vulnerability:
  - https://software.cisco.com/download/home
- 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.
- Use only licensed software and avoid to use/ download cracked or pirated software.
- Designate 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.