Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:127 **27-Jan-2021**

Threat Classification: Command Execution and Denial of Service (DOS)

Name: Multiple Vulnerabilities in Cisco RV110W, RV130, RV130W, and RV215W Routers

Affected Systems:

Affects the following Cisco Small Business routers:

- RV110W Wireless-N VPN Firewall
- RV130 VPN Router
- RV130W Wireless-N Multifunction VPN Router
- RV215W Wireless-N VPN Router

Summary:

There are multiple vulnerabilities in the Universal Plug and Play (UPnP) service and web-based management interface of Cisco Small Business **RV110W**, **RV130**, **RV130W**, and **RV215W** routers which may allow an attacker to execute arbitrary code or cause an affected device to restart unexpectedly. The web-based management interface of these devices is available through a local LAN connection, which cannot be disabled, or through the WAN connection if the remote management feature is enabled.

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

For more information, please find below official link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U

Recommendations:

- The Cisco Small Business **RV110W, RV130, RV130W, and RV215W** routers have entered the end-of-life process. It is advised to refer to the CISCO end-of-life notices for these products as: https://www.cisco.com/c/en/us/products/collateral/routers/small-business-rv-series-routers/eos-eol-notice-c51-742771.pdf

- Users are encouraged to migrate to the secure Routers series as per their requirement.

- When considering software upgrades, CISCO recommends to consult Cisco advisories available on the Cisco Security Advisories and Alerts page for determining the exposure and complete upgrade solution.

- Whenever required, 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 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.