Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:093 **28-July-2020**

Threat Classification: Code Execution

Name: CISCO Small Business Routers Remote Code Execution Vulnerability (CVE-2020-3323)

Affected Systems:

Affects the following products of CISCO Small Business Routers:

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

Summary:

This vulnerability is due to improper validation of user-supplied input in the web-based management interface which can exploited by sending crafted HTTP requests to the targeted system. A successful exploit could allow an attacker to execute arbitrary code as the root user on the underlying operating system of the affected device.

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-rce-AQKREqp

Recommendations:

- For detailed information of the fixed releases of CISCO Small Business Routers software for the aforementioned vulnerability, please visit following link:
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-AQKREqp#fs
- 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.
- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.
- In all cases, also ensure that devices to be upgraded to new release meet the requirements set by the vendor.
- 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.