CIRT.GY Guyana National Computer Incident Response Team

AL2022_40 Cisco has stated that it will not fix zero-day RCE in end-of-life VPN routers (20th June 2022)

Description

After revealing a remote code execution vulnerability that will not be patched, Cisco advises owners of end-of-life Small Business RV routers to upgrade to newer models.

Summary

This vulnerability is tracked as CVE-2022-20825 and impacts four small Business RV Series models, the RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router. A successful exploit could allow the attacker to execute arbitrary commands on an affected device using root-level privileges.

How it works

An attacker could exploit this vulnerability by sending a specially crafted request to the web-based management interface, resulting in root-level command execution.

The flaw exists due to the impacted devices' insufficient user input validation of incoming HTTP packets. This vulnerability only affects devices on WAN connections that have the web-based remote management interface enabled. While the remote management feature is not enabled by default, administrators should log in to the web-based management interface, navigate to "**Basic Settings** > **Remote Management**," and check the state of the relevant check box to see if remote management is enabled.

Remediation

Since the devices listed above are no longer supported by Cisco, the only mitigation is to disable remote management on the WAN interface to improve overall security and to upgrade to a newer model as soon as possible.

The Guyana National CIRT recommends that users and administrators review this update and apply it where necessary.

References

- *Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Remote Command Execution and Denial of Service Vulnerability*. (2022, June 15). Retrieved from Cisco Security Advisory. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-overflow-s2r82P9v
- Toulas, B. (2022, June 17). *Cisco says it won't fix zero-day RCE in end-of-life VPN routers*. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/cisco-says-it-won-t-fix-zero-day-rce-in-end-of-life-vpn-routers/