Critical CVE-2022-20825 in Cisco small business routers will not be fixed

bo borncity.com/win/2022/06/20/kritische-cve-2022-20825-in-cisco-small-business-routern-wird-nicht-gefixt

By guenni 2022-06-20

[German]A critical vulnerability CVE-2022-20825 exists in the RV110W, RV130, RV130W and RV215W small business routers, which has been assigned a CVE score of 9.8. Due to a lack of authentication, the vulnerability allows for remote command execution as well as denial of service attacks. The problem: The devices have fallen out of support for Cisco and no longer receive any security updates.

Vulnerability CVE-2022-20825

CVE-2022-20825 is a vulnerability located in the web-based management interface of the Cisco RV110W, RV130, RV130W and RV215W small business routers. This vulnerability could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to unexpectedly reboot, resulting in a denial of service (DoS) condition.

CSB RV110W Wireless Router, Source: Cisco

This vulnerability is due to insufficient validation of user input in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful attack could allow the attacker to execute arbitrary commands on an affected device with root privileges. Cisco has not released software updates to address this vulnerability.

Cisco doesn't patch

Cisco has published the security advisory Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Remote Command Execution and Denial of Service Vulnerability on June 15, 2022. There, the vulnerability is confirmed to be due to insufficient validation of user input on incoming HTTP packets. A successful attack could allow the attacker to execute arbitrary commands on an affected device with root privileges. Affected products are:

- RV110W Wireless-N VPN-Firewall
- RV130 VPN-Router
- RV130W Wireless-N Multifunktions-VPN-Router
- RV215W Drahtlos-N-VPN-Router

The web-based management interface of these devices is available via a local LAN connection that cannot be disabled. The function may also be addressable over a WAN connection if the remote management function is enabled. By default, the remote management feature is disabled on these devices. To determine if the remote management feature is enabled on a device, open the web-based management interface and select *Basic Settings > Remote Management*. If the *Enable* checkbox is selected, remote management is enabled on the device. There are no workarounds to mitigate this vulnerability, nor firmware updates to close it. The vendor writes:

> Cisco has not released and will not release software updates to address the vulnerability described in this advisory. The Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers have entered the end-of-life process.

So there will be no security updates either because the devices have fallen out of support. In other words: Those who use the routers mentioned will probably have to switch to new devices. (via)