CERT-EU

Security Advisory 2022-009

Critical Vulnerability in Cisco VPN Routers

February 7, 2022 — v1.0

TLP:WHITE

History:

- *07/02/2022 — v1.0 – Initial publication*

Summary

On January 4th, Cisco has issued advisories and software updates [1] to address multiple vulnerabilities of which the three most serious are identified as: `CVE-2022-20699`, `CVE-2022-20700`, `CVE-2022-20708` with a severity score of 10 out of 10.

- `CVE-2022-20699` could lead to Remote Code Execution by unauthenticated attackers with `root` privileges.
- `CVE-2022-20700` could allow a remote attacker to elevate privileges to `root`.
- `CVE-2022-20708` could allow an unauthenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system.

Concerning the `CVE-2022-20699` vulnerability, a public presentation has recently been done at the OffensiveCon2022 followed by a **leak of the exploit on Twitter** [2]. It is unknown what PoC exploits are available for the other vulnerabilities. However, once security updates are released, these PoCs tend to become publicly fairly quickly [3].

It is recommended to update as soon as possible.

Technical Details

The vulnerability `CVE-2022-20699` exists because HTTP requests are not properly validated in the management interface, according to Cisco. An attacker could exploit this vulnerability by sending malicious HTTP requests to the affected device that is acting as an SSL VPN Gateway.

The vulnerability `CVE-2022-20700` is due to flaws in the router's web-based management interface, which suffers from insufficient authorisation enforcement mechanisms.

The vulnerability `CVE-2022-20708` is due to insufficient validation of user-supplied input.

Affected Products

These vulnerabilities affect the following Cisco products:

`CVE-2022-20700` :

- RV160 VPN Routers
- RV160W Wireless-AC VPN Routers
- RV260 VPN Routers
- RV260P VPN Routers with PoE
- RV260W Wireless-AC VPN Routers

`CVE-2022-20699` & `CVE-2022-20708` :

- RV340 Dual WAN Gigabit VPN Routers
- RV340W Dual WAN Gigabit Wireless-AC VPN Routers
- RV345 Dual WAN Gigabit VPN Routers
- RV345P Dual WAN Gigabit POE VPN Routers

Recommendations

Cisco has released free software updates that address the vulnerabilities described in this advisory for the RV340 and RV345 Series. Cisco is working on fixes for the identified vulnerabilities for the RV160 and RV260 Series Routers as quickly as possible.

Cisco and CERT-EU strongly recommend upgrading Cisco routers to the latest version as soon as possible.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-mult-vuln-KA9PK6D

[2] https://twitter.com/RabbitPro/status/1489978906597859333

[3] https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-bugs-in-smb-routers-exploits-available/