Security Advisory 2022-059

Critical Vulnerabilities in Cisco VPN Routers

August 4, 2022 — v1.0

TLP:WHITE

History:

- *04/08/2022 — v1.0 – Initial publication*

Summary

On August 3, Cisco released a security advisory and patches regarding several critical vulnerabilities affecting Cisco VPN routers [1].

It is highly recommended upgrading affected appliances as soon as possible.

Technical Details

The following vulnerabilities are being addressed by the security advisory:

- **CVE-2022-20842**: Remote Code Execution and Denial of Service Vulnerability

This vulnerability, with a CVSS score of 9.8 out of 10, exists in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers and may allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface.

- **CVE-2022-20827**: Command Injection Vulnerability

This vulnerability, with a CVSS score of 9.0 out of 10, exists in the web filter database update feature of Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers and may allow an unauthenticated, remote attacker to perform a command injection and execute commands on the underlying operating system with root privileges. This vulnerability is due to insufficient input validation.

- **CVE-2022-20841**: Command Injection Vulnerability

This vulnerability, with a CVSS score of 8.3 out of 10, exists in the Open Plug and Play (PnP) module of Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system. This vulnerability is due to insufficient validation of user-supplied input.

Affected Products

CVE-2022-20827 and CVE-2022-20841:

- RV160 and RV260 Series Routers with version >= 1.0.01.05 and < 1.0.01.09 (1.0.01.09 is the first fixed release)
- RV340 and RV345 Series Routers with version >= 1.0.03.26 and < 1.0.03.28 (1.0.03.28 is the first fixed release)

CVE-2022-20842:

- RV340 and RV345 Series Routers with version 1.0.03.26 and earlier until 1.0.03.27 (1.0.03.28 is the first fixed release)

Recommendations

CERT-EU strongly recommends upgrading affected products to the last version available.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR