Security Advisory 2020-036

Critical Cisco Vulnerabilities

July 16, 2020 — v1.0

TLP:WHITE

History:

- *16/07/2020 — v1.0 – Initial publication*

Summary

Cisco released 31 Security Advisories for vulnerabilities affecting its products. Five of them are rated **critical** with **CVSS Score 9.8**. In particular, critical vulnerabilities affect: telnet service of firewall routers (CVE-2020-3330), web-based management interface of routers (CVE-2020-3323, CVE-2020-3144, and CVE-2020-3331), and web management interface of Cisco Prime License Manager (PLM) software (CVE-2020-3140) [1].

Technical Details

We present here on the details of the critical vulnerabilities. Additional information may be found in [1].

CVE-2020-3330

The vulnerability exists because a system account has a default and static password. An attacker could exploit this vulnerability by using this default account to connect to the affected system. A successful exploit could allow the attacker to gain full control of an affected device [2].

CVE-2020-3323

The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device [3].

CVE-2020-3144

The vulnerability is due to improper session management on affected devices. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to gain administrative access on the affected device [4].

CVE-2020-3331

The vulnerability is due to improper validation of user-supplied input data by the web-based management interface. An attacker could exploit this vulnerability by sending crafted requests

to a targeted device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the `root` user [5].

CVE-2020-3140

The vulnerability is due to insufficient validation of user input on the web management interface. An attacker could exploit this vulnerability by submitting a malicious request to an affected system. An exploit could allow the attacker to gain administrative-level privileges on the system. The attacker needs a valid username to exploit this vulnerability [6].

Products Affected

These vulnerabilities affect several products:

- RV110W Wireless-N VPN Firewall (CVE-2020-3323, CVE-2020-3144), and releases earlier than Release 1.2.2.8 (CVE-2020-3331)
- RV130 VPN Router (CVE-2020-3330, CVE-2020-3323, CVE-2020-3144)
- RV130W Wireless-N Multifunction VPN Router (CVE-2020-3330, CVE-2020-3323, CVE-2020-3144)
- RV215W Wireless-N VPN Router (CVE-2020-3330, CVE-2020-3323, CVE-2020-3144), and releases earlier than Release 1.3.1.7. (CVE-2020-3331)
- Cisco Prime License Manager 10.5(2)SU9 and earlier (CVE-2020-3140)
- Cisco Prime License Manager 11.5(1)SU6 and earlier (CVE-2020-3140)

Recommendations

Cisco has released software updates that address these vulnerabilities. **CERT-EU strongly advises applying available patches [1] as soon as possible**.

Workarounds

- For vulnerabilities identified by CVE-2020-3330, CVE-2020-3140, and CVE-2020-3331 there are no workarounds that address these vulnerabilities.
- For vulnerabilities identified by CVE-2020-3144 and CVE-2020-3323, there are also no workarounds. However, disabling the remote management feature (if it is not required) would help to reduce the attack surface.

References

[1] https://tools.cisco.com/security/center/publicationListing.x

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv110w-static-cred-BMTWBWTy

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-AQKREqp

[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-auth-bypass-cGv9EruZ

[5] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-code-exec-wH3BNFb

[6] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-prime-priv-esc-HyhwdzBA