CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-009

Critical Vulnerabilities in Cisco Products

February 4, 2021 — v1.0

TLP:WHITE

History:

- *04/02/2021 — v1.0 – Initial publication*

Summary

Cisco has published an advisory about several vulnerabilities affecting various Cisco Products [1-3]. These vulnerabilities could lead to **remote code execution**, **privilege escalation**, **directory traversal**, **file overwrite** or **denial of service**. While Cisco is not aware of any malicious exploit in the wild, it is highly recommended to patch the affected products.

Technical Details

This advisory only describes the most critical vulnerabilities disclosed by Cisco.

CVE-2021-1289, CVE-2021-1290, CVE-2021-1291

The first group of vulnerabilities, identified by **CVE-2021-1289**, **CVE-2021-1290** and **CVE-2021-1291** [1], exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. The CVSS score of these vulnerabilities is **9.8**

CVE-2021-1288, CVE-2021-1313

The first vulnerability of this group, identified by **CVE-2021-1288** [2], is due to a logic error that occurs when an affected device processes Telnet protocol packets. An attacker could exploit this vulnerability by sending specific streams of packets to the affected device. A successful exploit could allow the attacker to cause the `enf_broker` process to crash, which could lead to system instability and the inability to process or forward traffic through the affected device. The CVSS score of this vulnerability is **8.6**.

The second vulnerability, identified by **CVE-2021-1313** [2], is due to improper resource allocation when an affected device processes either ICMP or Telnet protocol packets. An attacker could exploit this vulnerability by sending specific streams of packets to the affected device. A successful exploit could allow the attacker to cause the `enf_broker` process to leak system memory. Over time, this memory leak could cause the `enf_broker` process to crash, which could lead

to system instability and the inability to process or forward traffic through the affected device. The CVSS score of this vulnerability is **8.6**.

CVE-2021-1296, CVE-2021-1297

These vulnerabilities, identified by **CVE-2021-1296** and **CVE-2021-1297** [3], are due to insufficient input validation in the web-based management interface of Cisco Small Business routers. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. The CVSS score of these vulnerabilities is **7.5**.

Affected products

The vulnerabilities **CVE-2021-1289**, **CVE-2021-1290**, **CVE-2021-1291**, **CVE-2021-1296** and **CVE-2021-1297** affect the following Cisco Small Business Routers if they are running a firmware release earlier than Release 1.0.01.02 [1,3]:

- RV160 VPN Router
- RV160W Wireless-AC VPN Router
- RV260 VPN Router
- RV260P VPN Router with POE
- RV260W Wireless-AC VPN Router

The following software released are vulnerable to at least one of the two vulnerabilities **CVE-2021-1288** and **CVE-2021-1313** [2]:

- Cisco IOS XR Software Release 5.0
- Cisco IOS XR Software Release 6.0, before 6.0.2

Recommendations

It is recommended to apply the patches from Cisco for all affected software and products.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dos-WwDdghs2

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn