Security Advisory 2020-052

Critical Cisco IOS XR Software Vulnerability Under Attack

October 21, 2020 — v1.0

TLP:WHITE

Summary

Cisco released a warning on the 20th of October regarding the attacks that are actively targeting the CVE-2020-3118 high severity vulnerability found to affect multiple carrier-grade routers that run the company's Cisco IOS XR Software [1]. An advisory for this vulnerability was released by Cisco in the 5th of February [2]. It is related to the Cisco Discovery Protocol implementation for Cisco IOS XR Software that could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device.

Technical Details

Attackers could exploit the vulnerability by sending a malicious Cisco Discovery Protocol packet to devices running a vulnerable IOS XR version. Successful exploitation could enable the attackers to trigger a stack overflow that could lead to arbitrary code execution with administrative privileges on the targeted device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages [1].

Even though this Cisco Discovery Protocol Format String Vulnerability could lead to remote code execution, it can only be exploited by unauthenticated adjacent attackers (Layer 2 adjacent) in the same broadcast domain as the vulnerable devices.

Products Affected

This vulnerability affect several Cisco products with the condition that they have Cisco Discovery Protocol enabled both globally and on at least one interface and if they are running a vulnerable release of Cisco IOS XR Software (32-bit or 64-bit):

- ASR 9000 Series Aggregation Services Routers
- Carrier Routing System (CRS)
- IOS XRv 9000 Router
- Network Convergence System (NCS) 540 Series Routers
- Network Convergence System (NCS) 560 Series Routers
- Network Convergence System (NCS) 1000 Series Routers
- Network Convergence System (NCS) 5000 Series Routers
- Network Convergence System (NCS) 5500 Series Routers
- Network Convergence System (NCS) 6000 Series Routers

This vulnerability also affects third-party white box routers if they have Cisco Discovery Protocol enabled both globally and on at least one interface and if they are running a vulnerable release of Cisco IOS XR Software.

Recommendations

Cisco has released software updates that address this vulnerability.

CERT-EU strongly advises applying available patches [2] as soon as possible.

Workarounds

There are no workarounds that address this vulnerability.

References

[1] https://www.bleepingcomputer.com/news/security/cisco-warns-of-attacks-targeting-high-severity-router-vulnerability/

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-iosxr-cdp-rce