CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-010

Severe Vulnerability in Cisco IOS XR Software

February 12, 2021 — v1.0

TLP:WHITE

History:

- *11/02/2021 — v1.0 – Initial publication*

Summary

Cisco has published an advisory about severe vulnerability affecting Cisco Cisco IOS XR Software. These vulnerabilities could allow an unauthenticated, remote attacker to cause a **denial of service (DoS) condition** on an affected device. Cisco is not aware of any malicious exploit in the wild [1].

Technical Details

The vulnerability is being tracked as CVE-2020-26070 and received CVSS - score of 8.6. It is triggered by improper resource allocation that occurs when an affected device processes network traffic in software switching mode. Hackers can weaponise the vulnerability by sending specific streams of Layer 3 or Layer 3 protocol data units (PDUs) to a vulnerable device [1,2].

If the attempt is successful, this could cause the machine to run out of buffer resources, making it unable to process or forward traffic. Successful exploit could lead to a denial-of-service (DoS) condition and and according to Cisco, device restart is needed [1].

When a device is experiencing buffer resources exhaustion, the following message may be seen in the system logs [1]:

```
%PKT_INFRA-spp-4-PKT_ALLOC_FAIL : Failed to allocate n packets for sending
```

This error message indicates that the device is not able to allocate buffer resources and forward network traffic in software switching mode [1,3].

Affected products

The vulnerability CVE-2020-26070 affects [1]:

- Cisco ASR 9000 Series Aggregation Services Routers
- Cisco Network Convergence System (NCS) 5000 Series Routers

Recommendations

Cisco has released free software updates that address the vulnerability described in the advisory.

It is recommended to install updates for the affected software.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xr-cp-dos-ej8VB9QY#fs

[2] https://sensorstechforum.com/cve-2020-26070-cisco-asr-routers-flaw/

[3] https://threatpost.com/high-severity-cisco-dos-flaw-asr-routers/161115/