CVE-2025-20115: CISCO IOS XR DENIAL OF SERVICE

Vairav CVE Report

Date: March 17th, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A vulnerability identified as **CVE-2025-20115** has been discovered in Cisco IOS XR Software. This flaw allows an unauthenticated, remote attacker to cause a denial-of-service (DoS) condition by crashing the Border Gateway Protocol (BGP) process. The vulnerability has been assigned a **CVSS score of 8.6**, categorized as **High** severity. Exploitation of this vulnerability could lead to service disruptions in networks utilizing affected versions of Cisco IOS XR Software.

VULNERABILITY DETAILS

CVE-2025-20115

- **Description:** This vulnerability arises from a memory corruption issue that occurs when a BGP update is created with an AS_CONFED_SEQUENCE attribute containing 255 autonomous system numbers (AS numbers). An attacker could exploit this vulnerability by sending a crafted BGP update message, leading to a crash of the BGP process on the affected device.
- **Impact:** Successful exploitation can result in a denial-of-service condition, disrupting BGP routing and potentially affecting network stability and data transmission.
- **CVSS Score:** 8.6 (High)

AFFECTED VERSIONS

All versions of Cisco IOS XR Software with BGP confederation configured are affected by this vulnerability.

EXPLOIT DETAILS

In environments where Cisco IOS XR Software is deployed for BGP routing, an attacker could exploit this vulnerability by sending a specially crafted BGP update message with an AS_CONFED_SEQUENCE attribute containing 255 AS numbers. This could lead to memory corruption and a subsequent crash of the BGP process, resulting in a denial-of-service

condition. Such an attack could disrupt network operations, leading to service outages and potential loss of connectivity.

RECOMMENDED ACTIONS

Patch & Upgrade: Cisco has released software updates to address this vulnerability. Administrators are advised to upgrade to the latest versions of Cisco IOS XR Software:

- **Cisco IOS XR Software version 24.2**: Upgrade to version 24.2.1
- **Cisco IOS XR Software version 24.3**: Upgrade to version 24.3.1

ADDITIONAL SECURITY MEASURES

- **Access Control**: Implement robust access control lists (ACLs) to limit BGP connections to trusted peers only, reducing the risk of unauthorized or malicious BGP updates.
- **Monitoring**: Continuously monitor BGP sessions and logs for any unusual activity or malformed BGP update messages that could indicate exploitation attempts.
- **Network Segmentation**: Segment network infrastructure to limit the impact of a potential BGP process crash, ensuring that critical services remain operational.

REFERENCES

- https://securityaffairs.com/175421/security/cisco-ios-xr-flaw-cve-2025-20115.html
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-bgp-dos-O7stePhX#fs

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com