February 28, 2024

**Overall Rating - High**

**This notification is intended as an informational bulletin for technical audiences.**

## Summary

The Vulnerability and Risk Management (VRM) Team is aware that Cisco published security advisories to address vulnerabilities in the following product:

- Cisco NX-OS - multiple platforms and versions

## Technical Details

A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.
This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network.

These vulnerabilities are rated as an overall **High** Severity.

## Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

## References

- CVE-2024-20321 CVE-2024-20267 CVE-2024-20344 CVE-2024-20291 CVE-2024-20294
- Cisco Advisory – cisco-sa-nxos-ebgp-dos-L3QCwVJ
- Cisco Advisory – cisco-sa-ipv6-mpls-dos-R9ycXkwM
- Cisco Security Advisories