Advisory Alert

Alert Number: AAA20221223 **Date:** December 23, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**High**	Input Validation vulnerability

Description

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Input Validation vulnerability (CVE-2022-22184)
Description	Juniper has released a security update to address an improper input validation vulnerability in their Routing Protocol Daemon for Juniper Networks' Junos OS and Junos OS Evolved. A remote attacker could exploit this vulnerability by sending continuous BGP update messages with specific optional transitive attributes over an established BGP session, resulting in sustained Denial of Service. Juniper recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Juniper Networks Junos OS version 22.3R1. Juniper Networks Junos OS Evolved version 22.3R1-EVO.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2022-12-Out-of-Cycle-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-BGP-session-will-flap-upon-receipt-of-a-specific-optional-transitive-attribute-in-version-22-3R1-CVE-2022-22184?language=en_US

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.