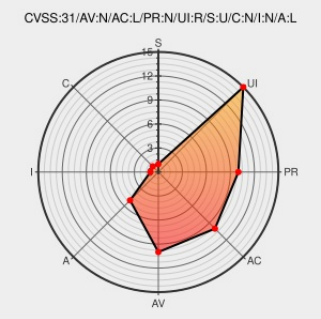
CVE-2020-3449

Published on: 08/17/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:39 PM UTC

CVE-2020-3449 - advisory for cisco-sa-bgp-ErKEqAer

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ios Xr from Cisco contain the following vulnerability:

A vulnerability in the Border Gateway Protocol (BGP) additional paths feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to prevent authorized users from monitoring the BGP status and cause the BGP process to stop processing new updates, resulting in a denial of service (DOS) condition. The vulnerability is due to an incorrect calculation of lexicographical order when displaying additional path information within Cisco IOS XR Software, which causes an infinite loop. An attacker could exploit this vulnerability by sending a specific BGP update from a BGP neighbor peer session of an affected device; an authorized user must then issue a show bgp command for the vulnerability to be exploited. A successful exploit could allow the attacker to prevent authorized users from properly monitoring the BGP status and prevent BGP from processing new updates, resulting in outdated information in the routing and forwarding tables.

CVE-2020-3449 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco IOS XR Software** version **n/a**

CVSS3 Score: 4.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	LOW

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication

Vector	Complexity	
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Cisco IOS XR Software Additional Paths Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200805 Cisco IOS XR Software Additional Paths Denial of Service Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios Xr	All	All	All	All
Operating System	Cisco	Ios Xr	All	All	All	All

cpe:2.3:o:cisco:ios_xr:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xr:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→