CVE-2017-12319

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-12319
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-27 09:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the Border Gateway Protocol (BGP) over an Ethernet Virtual Private Network (EVPN) for Cisco IOS XE Sc

Risk And Classification

EPSS: 0.012690000 probability, percentile 0.796620000 (date 2026-05-14)

CISA KEV: Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

Problem Types: CWE-20

CISA Known Exploited Vulnerability

Vendor	Cisco
Product	IOS XE Software
Name	Cisco IOS XE Software Ethernet Virtual Private Network Border Gateway Protocol Denial-of-Service Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-12319

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios	15.4(1)s	All	All	All
Operating System	Cisco	Ios	15.4\(1\)s	All	All	All
Operating System	Cisco	Ios	15.4\(1\)s	All	All	All
Operating System	Cisco	Ios Xe	All	All	All	All
Operating System	Cisco	Ios Xe	All	All	All	All

References

Reference	Source	Link

Reference	Source	Link
Cisco IOS XE Software CVE-2017-12319 Denial of Service Vulnerability	BID	www.security
Cisco IOS XE Software Ethernet Virtual Private Network Border Gateway Protocol Denial of Service Vulnerability	CONFIRM	tools.cisco.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.go

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**