



CVE-2009-2049

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2009-2049
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-30 18:30:00 UTC
Updated	2017-09-29 01:34:00 UTC
Description	Cisco IOS 12.0(32)S12 through 12.0(32)S13 and 12.0(33)S3 through 12.0(33)S4, 12.0(32)SY8 through 12.0(32)SY9, 12.2(

Risk And Classification

Problem Types: CWE-16

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios	12.0(32)s12	All	All	All
Operating System	Cisco	ios	12.0(32)s13	All	All	All
Operating System	Cisco	ios	12.0(32)sy8	All	All	All
Operating System	Cisco	ios	12.0(32)sy9	All	All	All
Operating System	Cisco	ios	12.0(33)s3	All	All	All
Operating System	Cisco	ios	12.0(33)s4	All	All	All
Operating System	Cisco	ios	12.0(32)s12	All	All	All
Operating System	Cisco	ios	12.0(32)s13	All	All	All
Operating System	Cisco	ios	12.0(32)sy8	All	All	All
Operating System	Cisco	ios	12.0(32)sy9	All	All	All
Operating System	Cisco	ios	12.0(33)s3	All	All	All
Operating System	Cisco	ios	12.0(33)s4	All	All	All
Operating System	Cisco	ios	12.2(33)sxi1	All	All	All
Operating System	Cisco	ios	12.2(33)sxi2	All	All	All
Operating System	Cisco	ios	12.2xnc	All	All	All
Operating System	Cisco	ios	12.2xnd	All	All	All
Operating System	Cisco	ios	12.2(33)sxi1	All	All	All

Operating System	Cisco	ios	12.2\33\)\sxi2	All	All	All
Operating System	Cisco	ios	12.4(24)t1	All	All	All
Operating System	Cisco	ios	12.4(24)\t1	All	All	All
Operating System	Cisco	ios	12.0(32)\s12	All	All	All
Operating System	Cisco	ios	12.0(32)\s13	All	All	All
Operating System	Cisco	ios	12.0(32)\sy8	All	All	All
Operating System	Cisco	ios	12.0(32)\sy9	All	All	All
Operating System	Cisco	ios	12.0(33)\s3	All	All	All
Operating System	Cisco	ios	12.0(33)\s4	All	All	All
Operating System	Cisco	ios	12.2xnc	All	All	All
Operating System	Cisco	ios	12.2xnd	All	All	All
Operating System	Cisco	ios	12.2(33)\sxi1	All	All	All
Operating System	Cisco	ios	12.2(33)\sxi2	All	All	All
Operating System	Cisco	ios	12.4(24)\t1	All	All	All
Operating System	Cisco	ios Xe	2.3	All	All	All
Operating System	Cisco	ios Xe	2.3.1t	All	All	All
Operating System	Cisco	ios Xe	2.4	All	All	All
Operating System	Cisco	ios Xe	2.4.0	All	All	All
Operating System	Cisco	ios Xe	2.3	All	All	All
Operating System	Cisco	ios Xe	2.3.1t	All	All	All
Operating System	Cisco	ios Xe	2.4	All	All	All
Operating System	Cisco	ios Xe	2.4.0	All	All	All

References

Reference

Cisco IOS 4-Byte ASN Support Bugs in Processing BGP Updates Let Remote Users Deny Service - SecurityTracker

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Cisco Security Advisory: Cisco IOS Software Border Gateway Protocol 4-Byte Autonomous System Number Vulnerabilities - Cisco Systems

Repository / Oval Repository

Cisco IOS Border Gateway Protocol Two Denial of Service Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

Cisco IOS Malformed Border Gateway Protocol Update Denial of Service Vulnerability

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)