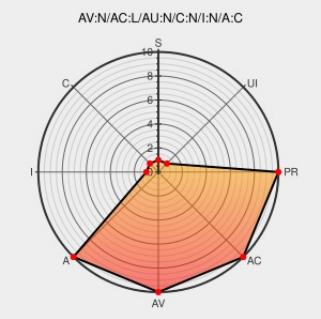
CVE-2009-2870

Published on: 09/28/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:30 PM UTC

CVE-2009-2870

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



Certain versions of Ios from Cisco contain the following vulnerability:

Unspecified vulnerability in Cisco IOS 12.2 through 12.4, when the Cisco Unified Border Element feature is enabled, allows remote attackers to cause a denial of service (device reload) via crafted SIP messages, aka Bug ID CSCsx25880.

CVE-2009-2870 has been assigned by psirt@cisco.com to track the vulnerability

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Cisco IOS H.323, SIP, NTP, Tunneling, and Encrypted Packet Processing Flaws Let Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1022930
Cisco Security Advisory: Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability - Cisco Systems	Vendor Advisory www.cisco.com text/html	CISCO 20090923 Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability
No Description Provided	Vendor Advisory tools.cisco.com text/html	CONFIRM tools.cisco.com/security/center/viewAlert.x?alertId=18891
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	VUPEN ADV-2009-2759

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	12.3yk	All	All	All
Operating System	Cisco	Ios	12.3ys	All	All	All
Operating System	Cisco	Ios	12.3yt	All	All	All
Operating System	Cisco	Ios	12.4gc	All	All	All
Operating System	Cisco	Ios	12.4mr	All	All	All
Operating System	Cisco	Ios	12.4t	All	All	All
Operating System	Cisco	Ios	12.4xa	All	All	All
Operating System	Cisco	Ios	12.4xc	All	All	All
Operating System	Cisco	Ios	12.4xd	All	All	All
Operating System	Cisco	Ios	12.4xe	All	All	All
Operating System	Cisco	Ios	12.4xl	All	All	All
Operating System	Cisco	Ios	12.4xm	All	All	All
Operating System	Cisco	Ios	12.4xp	All	All	All
Operating System	Cisco	Ios	12.4xt	All	All	All
Operating System	Cisco	Ios	12.4xv	All	All	All
Operating System	Cisco	Ios	12.4xw	All	All	All
Operating System	Cisco	Ios	12.4xy	All	All	All
Operating System	Cisco	Ios	12.4xz	All	All	All
Operating System	Cisco	Ios	12.4ya	All	All	All

System						
Operating System	Cisco	Ios	12.3yk	All	All	All
Operating System	Cisco	Ios	12.3ys	All	All	All
Operating System	Cisco	Ios	12.3yt	All	All	All
Operating System	Cisco	Ios	12.4gc	All	All	All
Operating System	Cisco	Ios	12.4mr	All	All	All
Operating System	Cisco	Ios	12.4t	All	All	All
Operating System	Cisco	Ios	12.4xa	All	All	All
Operating System	Cisco	Ios	12.4xc	All	All	All
Operating System	Cisco	Ios	12.4xd	All	All	All
Operating System	Cisco	Ios	12.4xe	All	All	All
Operating System	Cisco	Ios	12.4xl	All	All	All
Operating System	Cisco	Ios	12.4xm	All	All	All
Operating System	Cisco	Ios	12.4xp	All	All	All
Operating System	Cisco	Ios	12.4xt	All	All	All
Operating System	Cisco	Ios	12.4xv	All	All	All
Operating System	Cisco	Ios	12.4xw	All	All	All
Operating System	Cisco	Ios	12.4xy	All	All	All
Operating System	Cisco	Ios	12.4xz	All	All	All
Operating System	Cisco	Ios	12.4ya	All	All	All

cpe:2.3:o:cisco:ios:12.3yk:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.3ys:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.3yt:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4gc:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4mr:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xa:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xc:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xd:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xe:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xl:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xm:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xp:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xt:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xv:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xw:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xy:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xz:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4ya:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.3yk:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.3ys:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.3yt:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4gc:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4mr:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xa:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xc:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xd:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xe:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xl:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xm:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xp:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xt:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xv:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xw:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xy:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4xz:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:12.4ya:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→