



CVE-2011-3275

Published on: 10/03/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:14 PM UTC

CVE-2011-3275

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [ios](#) from [Cisco](#) contain the following vulnerability:

Memory leak in Cisco IOS 12.4, 15.0, and 15.1, and IOS XE 2.5.x through 3.2.x, allows remote attackers to cause a denial of service (memory consumption) via a crafted SIP message, aka Bug ID CSCti48504.

CVE-2011-3275 has been assigned by [cisco](#) psirt@cisco.com to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Alert Details - Security Center - Cisco Systems

[tools.cisco.com](#)
[text/html](#)

CONFIRM [tools.cisco.com/security/center/viewAlert.x?alertId=24130](#)

Cisco Systems - Redirect to

[Vendor Advisory](#)
[www.cisco.com](#)
[text/html](#)

CISCO 20110928 Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities

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	12.4	All	All	All
Operating System	Cisco	ios	15.0	All	All	All
Operating System	Cisco	ios	15.1	All	All	All
Operating System	Cisco	ios	12.4	All	All	All
Operating System	Cisco	ios	15.0	All	All	All
Operating System	Cisco	ios	15.1	All	All	All
Operating System	Cisco	ios Xe	2.5.0	All	All	All
Operating System	Cisco	ios Xe	2.5.1	All	All	All
Operating System	Cisco	ios Xe	2.5.2	All	All	All
Operating System	Cisco	ios Xe	2.6.0	All	All	All
Operating System	Cisco	ios Xe	2.6.1	All	All	All
Operating System	Cisco	ios Xe	2.6.2	All	All	All
Operating System	Cisco	ios Xe	3.1.0s	All	All	All
Operating System	Cisco	ios Xe	3.1.1s	All	All	All
Operating System	Cisco	ios Xe	3.1.2s	All	All	All
Operating System	Cisco	ios Xe	3.1.3s	All	All	All
Operating System	Cisco	ios Xe	3.1.4s	All	All	All
Operating System	Cisco	ios Xe	3.2.0s	All	All	All
Operating System	Cisco	ios Xe	3.2.1s	All	All	All
Operating System	Cisco	ios Xe	3.2.2s	All	All	All
Operating System	Cisco	ios Xe	2.5.0	All	All	All
Operating System	Cisco	ios Xe	2.5.1	All	All	All

Operating System	Cisco	ios Xe	2.5.1	All	All	All
Operating System	Cisco	ios Xe	2.5.2	All	All	All
Operating System	Cisco	ios Xe	2.6.0	All	All	All
Operating System	Cisco	ios Xe	2.6.1	All	All	All
Operating System	Cisco	ios Xe	2.6.2	All	All	All
Operating System	Cisco	ios Xe	3.1.0s	All	All	All
Operating System	Cisco	ios Xe	3.1.1s	All	All	All
Operating System	Cisco	ios Xe	3.1.2s	All	All	All
Operating System	Cisco	ios Xe	3.1.3s	All	All	All
Operating System	Cisco	ios Xe	3.1.4s	All	All	All
Operating System	Cisco	ios Xe	3.2.0s	All	All	All
Operating System	Cisco	ios Xe	3.2.1s	All	All	All
Operating System	Cisco	ios Xe	3.2.2s	All	All	All
cpe:2.3:o:cisco:ios:12.4:*****:						
cpe:2.3:o:cisco:ios:15.0:*****:						
cpe:2.3:o:cisco:ios:15.1:*****:						
cpe:2.3:o:cisco:ios:12.4:*****:						
cpe:2.3:o:cisco:ios:15.0:*****:						
cpe:2.3:o:cisco:ios:15.1:*****:						
cpe:2.3:o:cisco:ios_xe:2.5.0:*****:						
cpe:2.3:o:cisco:ios_xe:2.5.1:*****:						
cpe:2.3:o:cisco:ios_xe:2.5.2:*****:						
cpe:2.3:o:cisco:ios_xe:2.6.0:*****:						
cpe:2.3:o:cisco:ios_xe:2.6.1:*****:						
cpe:2.3:o:cisco:ios_xe:2.6.2:*****:						
cpe:2.3:o:cisco:ios_xe:3.1.0s:*****:						

cpe:2.3:o:cisco:ios_xe:3.1.1s:*****:
cpe:2.3:o:cisco:ios_xe:3.1.2s:*****:
cpe:2.3:o:cisco:ios_xe:3.1.3s:*****:
cpe:2.3:o:cisco:ios_xe:3.1.4s:*****:
cpe:2.3:o:cisco:ios_xe:3.2.0s:*****:
cpe:2.3:o:cisco:ios_xe:3.2.1s:*****:
cpe:2.3:o:cisco:ios_xe:3.2.2s:*****:
cpe:2.3:o:cisco:ios_xe:2.5.0:*****:
cpe:2.3:o:cisco:ios_xe:2.5.1:*****:
cpe:2.3:o:cisco:ios_xe:2.5.2:*****:
cpe:2.3:o:cisco:ios_xe:2.6.0:*****:
cpe:2.3:o:cisco:ios_xe:2.6.1:*****:
cpe:2.3:o:cisco:ios_xe:2.6.2:*****:
cpe:2.3:o:cisco:ios_xe:3.1.0s:*****:
cpe:2.3:o:cisco:ios_xe:3.1.1s:*****:
cpe:2.3:o:cisco:ios_xe:3.1.2s:*****:
cpe:2.3:o:cisco:ios_xe:3.1.3s:*****:
cpe:2.3:o:cisco:ios_xe:3.1.4s:*****:
cpe:2.3:o:cisco:ios_xe:3.2.0s:*****:
cpe:2.3:o:cisco:ios_xe:3.2.1s:*****:
cpe:2.3:o:cisco:ios_xe:3.2.2s:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

[site](#). This site includes MITRE data granted under the following [license](#).

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