

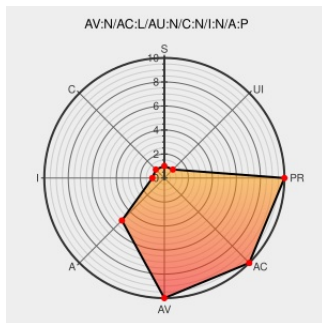


CVE-2004-0710

Published on: 07/21/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:11 PM UTC

CVE-2004-0710

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

Certain versions of [ios](#) from [Cisco](#) contain the following vulnerability:
IP Security VPN Services Module (VPNSM) in Cisco Catalyst 6500 Series Switch and the Cisco 7600 Series Internet Routers running IOS before 12.2(17b)SXA, before 12.2(17d)SXB, or before 12.2(14)SY03 could allow remote attackers to cause a denial of service (device crash and reload) via a malformed Internet Key Exchange (IKE) packet.

CVE-2004-0710 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

[OVAL oval:org.mitre.oval:def:5696](#)

Cisco IOS Malformed IKE Packet Remote Denial
Of Service Vulnerability

[Vendor Advisory](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 10083](#)

US-CERT Vulnerability Note VU#904310

[Third Party Advisory](#)
[US Government Resource](#)
[www.kb.cert.org](#)
[text/html](#)

[CERT-VN VU#904310](#)

Cisco - Networking, Cloud, and Cybersecurity
Solutions

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

[CISCO 20040408 Cisco IPSec VPN Services
Module Malformed IKE Packet Vulnerability](#)

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	12.2(14)sy	All	All	All
Operating System	Cisco	ios	12.2(14)za	All	All	All
Operating System	Cisco	ios	12.2(14)za2	All	All	All
Operating System	Cisco	ios	12.2(17a)sxa	All	All	All
Operating System	Cisco	ios	12.2sxa	All	All	All
Operating System	Cisco	ios	12.2sxb	All	All	All
Operating System	Cisco	ios	12.2sy	All	All	All
Operating System	Cisco	ios	12.2za	All	All	All
Operating System	Cisco	ios	12.2\14\sy	All	All	All
Operating System	Cisco	ios	12.2\14\za	All	All	All
Operating System	Cisco	ios	12.2\14\za2	All	All	All
Operating System	Cisco	ios	12.2\17a\sxa	All	All	All
Operating System	Cisco	ios	12.2sxa	All	All	All
Operating System	Cisco	ios	12.2sxb	All	All	All
Operating System	Cisco	ios	12.2sy	All	All	All
Operating System	Cisco	ios	12.2za	All	All	All
Operating System	Cisco	ios	12.2\14\sy	All	All	All

Operating System	Cisco	ios	12.2\14\za	All	All	All
Operating System	Cisco	ios	12.2\14\za2	All	All	All
Operating System	Cisco	ios	12.2\17a\sxa	All	All	All
cpe:2.3:o:cisco:ios:12.2(14)sy:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2(14)za:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2(14)za2:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2(17a)sxa:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2sxa:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2sxb:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2sy:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2za:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2\14\sy:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2\14\za:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2\14\za2:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2\17a\sxa:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2sxa:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2sxb:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2sy:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2za:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2\14\sy:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2\14\za:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2\14\za2:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:cisco:ios:12.2\17a\sxa:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#).

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