

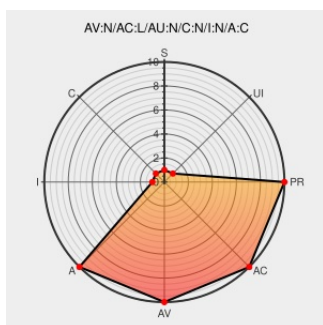


CVE-2008-2739

Published on: 09/26/2008 12:00:00 AM UTC

Last Modified on: 06/02/2022 05:09:00 PM UTC

CVE-2008-2739

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

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

The SERVICE.DNS signature engine in the Intrusion Prevention System (IPS) in Cisco IOS 12.3 and 12.4 allows remote attackers to cause a denial of service (device crash or hang) via network traffic that triggers unspecified IPS signatures, a different vulnerability than CVE-2008-1447.

CVE-2008-2739 has been assigned by [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

Cisco IOS Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

[web.archive.org](#)
[text/html](#)

[X SECUNIA 31990](#)

Cisco Security Advisory: Cisco IOS IPS Denial of Service Vulnerability - Cisco Systems

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

[CISCO 20080924 Cisco IOS IPS Denial of Service Vulnerability](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2008-2670](#)

Repository / Oval Repository

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

[OVAL oval.org.mitre.oval:def:6058](#)

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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware  	Cisco	ios	12.3t	All	All	All
Hardware  	Cisco	ios	12.3xl	All	All	All
Hardware  	Cisco	ios	12.3xq	All	All	All
Hardware  	Cisco	ios	12.3xr	All	All	All
Hardware  	Cisco	ios	12.3xs	All	All	All
Hardware  	Cisco	ios	12.3xx	All	All	All
Hardware  	Cisco	ios	12.3ya	All	All	All
Hardware  	Cisco	ios	12.3yd	All	All	All
Hardware  	Cisco	ios	12.3yg	All	All	All
Hardware  	Cisco	ios	12.3yh	All	All	All
Hardware  	Cisco	ios	12.3yk	All	All	All
Hardware  	Cisco	ios	12.3ys	All	All	All
Hardware  	Cisco	ios	12.3yt	All	All	All
Hardware  	Cisco	ios	12.3za	All	All	All
Hardware  	Cisco	ios	12.4xa	All	All	All
Hardware  	Cisco	ios	12.4xc	All	All	All
Hardware  	Cisco	ios	12.4xe	All	All	All
Hardware  	Cisco	ios	12.4xj	All	All	All
Hardware  	Cisco	ios	12.4xk	All	All	All
Hardware  	Cisco	ios	12.4xt	All	All	All
Hardware  	Cisco	ios	12.4xv	All	All	All
Operating System	Cisco	ios	12.3t	All	All	All
Operating System	Cisco	ios	12.3xl	All	All	All
Operating System	Cisco	ios	12.3xq	All	All	All
Operating System	Cisco	ios	12.3xr	All	All	All

Operating System	Cisco	los	12.3xs	All	All	All
Operating System	Cisco	los	12.3xx	All	All	All
Operating System	Cisco	los	12.3ya	All	All	All
Operating System	Cisco	los	12.3yd	All	All	All
Operating System	Cisco	los	12.3yg	All	All	All
Operating System	Cisco	los	12.3yh	All	All	All
Operating System	Cisco	los	12.3yi	All	All	All
Operating System	Cisco	los	12.3yk	All	All	All
Operating System	Cisco	los	12.3ys	All	All	All
Operating System	Cisco	los	12.3yt	All	All	All
Operating System	Cisco	los	12.3za	All	All	All
Operating System	Cisco	los	12.4xa	All	All	All
Operating System	Cisco	los	12.4xc	All	All	All
Operating System	Cisco	los	12.4xe	All	All	All
Operating System	Cisco	los	12.4xf	All	All	All
Operating System	Cisco	los	12.4xj	All	All	All
Operating System	Cisco	los	12.4xk	All	All	All
Operating System	Cisco	los	12.4xt	All	All	All
Operating System	Cisco	los	12.4xv	All	All	All
Hardware  	Cisco	los	12.3t	All	All	All
Hardware  	Cisco	los	12.3xl	All	All	All
Hardware  	Cisco	los	12.3xq	All	All	All
Hardware  	Cisco	los	12.3xr	All	All	All
Hardware  	Cisco	los	12.3xs	All	All	All

Hardware	Cisco	ios	12.3xx	All	All	All
Hardware	Cisco	ios	12.3ya	All	All	All
Hardware	Cisco	ios	12.3yd	All	All	All
Hardware	Cisco	ios	12.3yg	All	All	All
Hardware	Cisco	ios	12.3yh	All	All	All
Hardware	Cisco	ios	12.3yk	All	All	All
Hardware	Cisco	ios	12.3ys	All	All	All
Hardware	Cisco	ios	12.3yt	All	All	All
Hardware	Cisco	ios	12.3za	All	All	All
Hardware	Cisco	ios	12.4xa	All	All	All
Hardware	Cisco	ios	12.4xc	All	All	All
Hardware	Cisco	ios	12.4xe	All	All	All
Hardware	Cisco	ios	12.4xj	All	All	All
Hardware	Cisco	ios	12.4xk	All	All	All
Hardware	Cisco	ios	12.4xt	All	All	All
Hardware	Cisco	ios	12.4xv	All	All	All
Operating System	Cisco	ios	12.3yi	All	All	All
Operating System	Cisco	ios	12.4xf	All	All	All
cpe:2.3:h:cisco:ios:12.3t:*****:						
cpe:2.3:h:cisco:ios:12.3xl:*****:						
cpe:2.3:h:cisco:ios:12.3xq:*****:						
cpe:2.3:h:cisco:ios:12.3xr:*****:						
cpe:2.3:h:cisco:ios:12.3xs:*****:						
cpe:2.3:h:cisco:ios:12.3xx:*****:						
cpe:2.3:h:cisco:ios:12.3ya:*****:						
cpe:2.3:h:cisco:ios:12.3yd:*****:						
cpe:2.3:h:cisco:ios:12.3yg:*****:						
cpe:2.3:h:cisco:ios:12.3yh:*****:						
cpe:2.3:h:cisco:ios:12.3yk:*****:						
cpe:2.3:h:cisco:ios:12.3ys:*****:						

cpe:2.3:h:cisco:ios:12.3ys:~::~:
cpe:2.3:h:cisco:ios:12.3yt:~::~:
cpe:2.3:h:cisco:ios:12.3za:~::~:
cpe:2.3:h:cisco:ios:12.4xa:~::~:
cpe:2.3:h:cisco:ios:12.4xc:~::~:
cpe:2.3:h:cisco:ios:12.4xe:~::~:
cpe:2.3:h:cisco:ios:12.4xj:~::~:
cpe:2.3:h:cisco:ios:12.4xk:~::~:
cpe:2.3:h:cisco:ios:12.4xt:~::~:
cpe:2.3:h:cisco:ios:12.4xv:~::~:
cpe:2.3:o:cisco:ios:12.3t:~::~:
cpe:2.3:o:cisco:ios:12.3xl:~::~:
cpe:2.3:o:cisco:ios:12.3xq:~::~:
cpe:2.3:o:cisco:ios:12.3xr:~::~:
cpe:2.3:o:cisco:ios:12.3xs:~::~:
cpe:2.3:o:cisco:ios:12.3xx:~::~:
cpe:2.3:o:cisco:ios:12.3ya:~::~:
cpe:2.3:o:cisco:ios:12.3yd:~::~:
cpe:2.3:o:cisco:ios:12.3yg:~::~:
cpe:2.3:o:cisco:ios:12.3yh:~::~:
cpe:2.3:o:cisco:ios:12.3yi:~::~:
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:12.3za:~::~:
cpe:2.3:o:cisco:ios:12.4xa:~::~:
cpe:2.3:o:cisco:ios:12.4xc:~::~:
cpe:2.3:o:cisco:ios:12.4xe:~::~:
cpe:2.3:o:cisco:ios:12.4xf:~::~:

[← Previous ID](#)[Next ID→](#)

© [CVE.report](#) 2023   |

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](#).

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