

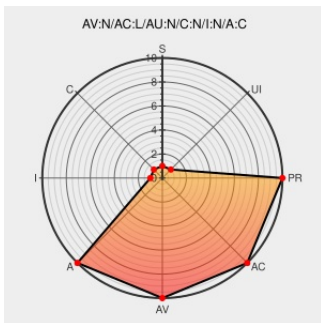


CVE-2009-2871

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

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

CVE-2009-2871

[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 and 12.4, when SSLVPN sessions, SSH sessions, or IKE encrypted nonces are enabled, allows remote attackers to cause a denial of service (device reload) via a crafted encrypted packet, aka Bug ID CSCsq24002.

CVE-2009-2871 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

Cisco IOS H.323, SIP, NTP, Tunneling, and Encrypted Packet Processing Flaws Let Remote Users Deny Service - SecurityTracker

www.securitytracker.com
text/html

[SECTRAK 1022930](#)

No Description Provided

Vendor Advisory
tools.cisco.com
text/html

[CONFIRM](#)
tools.cisco.com/security/center/viewAlert.x?alertId=18892

Cisco Security Advisory: Cisco IOS Software Crafted Encryption Packet Denial of Service Vulnerability [Products & Services] - Cisco Systems

Vendor Advisory
www.cisco.com
text/html

[CISCO 20090923 Cisco IOS Software Crafted Encryption Packet Denial of Service Vulnerability](#)

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

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	12.2xna	All	All	All
Operating System	Cisco	ios	12.2xnb	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	12.4md	All	All	All
Operating System	Cisco	ios	12.4mr	All	All	All
Operating System	Cisco	ios	12.4sw	All	All	All
Operating System	Cisco	ios	12.4t	All	All	All
Operating System	Cisco	ios	12.4xf	All	All	All
Operating System	Cisco	ios	12.4xj	All	All	All
Operating System	Cisco	ios	12.4xk	All	All	All
Operating System	Cisco	ios	12.4xq	All	All	All
Operating System	Cisco	ios	12.4xr	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	12.2xna	All	All	All
Operating System	Cisco	ios	12.2xnb	All	All	All

System						
Operating System	Cisco	ios	12.2xnc	All	All	All
Operating System	Cisco	ios	12.2xnd	All	All	All
Operating System	Cisco	ios	12.4md	All	All	All
Operating System	Cisco	ios	12.4mr	All	All	All
Operating System	Cisco	ios	12.4sw	All	All	All
Operating System	Cisco	ios	12.4t	All	All	All
Operating System	Cisco	ios	12.4xf	All	All	All
Operating System	Cisco	ios	12.4xj	All	All	All
Operating System	Cisco	ios	12.4xk	All	All	All
Operating System	Cisco	ios	12.4xq	All	All	All
Operating System	Cisco	ios	12.4xr	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
cpe:2.3:o:cisco:ios:12.2xna:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.2xnb:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.2xnc:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.2xnd:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.4md:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.4mr:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.4sw:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.4t:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.4xf:*:*:*:*:*:						

```
cpe:2.3:o:cisco:ios:12.4xj:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.4xk:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.4xq:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.4xr:*.:*:*:*:*:*:
```

```
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:12.2xna:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.2xnb:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.2xnc:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.2xnd:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.4md:*:*:*:*:*:
```

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

```
cpe:2.3:o:cisco:ios:12.4sw:*:*:*:*:*:*:
```

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

```
cpe:2.3:o:cisco:ios:12.4xf:*.:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.4xj:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.4xk:*.:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.4xq:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.4xr:*:*:*:*:*:
```

```
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:*.:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

[← 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](#)