

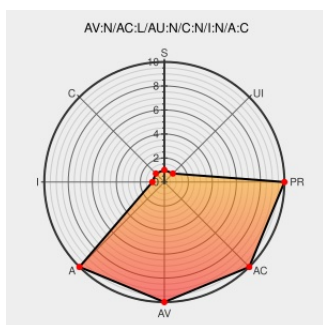


CVE-2009-2868

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

Last Modified on: 03/23/2021 11:25:31 PM UTC

CVE-2009-2868

[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 certificate-based authentication is enabled for IKE, allows remote attackers to cause a denial of service (Phase 1 SA exhaustion) via crafted requests, aka Bug IDs CSCsy07555 and CSCee72997.

CVE-2009-2868 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 Security Advisory: Cisco IOS Software Internet Key Exchange Resource Exhaustion Vulnerability - Cisco Systems

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

[CISCO 20090923 Cisco IOS Software Internet Key Exchange Resource Exhaustion Vulnerability](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

[VUPEN ADV-2009-2759](#)

No Description Provided

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

[CONFIRM](#)
[tools.cisco.com/security/center/viewAlert.x?alertId=18887](#)

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	12.2ex	All	All	All
Operating System	Cisco	ios	12.2ira	All	All	All
Operating System	Cisco	ios	12.2irb	All	All	All
Operating System	Cisco	ios	12.2irc	All	All	All
Operating System	Cisco	ios	12.2sb	All	All	All
Operating System	Cisco	ios	12.2sca	All	All	All
Operating System	Cisco	ios	12.2scb	All	All	All
Operating System	Cisco	ios	12.2se	All	All	All
Operating System	Cisco	ios	12.2sra	All	All	All
Operating System	Cisco	ios	12.2srb	All	All	All
Operating System	Cisco	ios	12.2src	All	All	All
Operating System	Cisco	ios	12.2srd	All	All	All
Operating System	Cisco	ios	12.2sxh	All	All	All
Operating System	Cisco	ios	12.2sxi	All	All	All
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	12.3t	All	All	All
Operating System	Cisco	ios	12.3xl	All	All	All

Operating System	Cisco	los	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	12.3yf	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	12.3yq	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	12.3yu	All	All	All
Operating System	Cisco	los	12.3yx	All	All	All
Operating System	Cisco	los	12.3yz	All	All	All
Operating System	Cisco	los	12.4	All	All	All
Operating System	Cisco	los	12.4t	All	All	All
Operating System	Cisco	los	12.4xb	All	All	All
Operating System	Cisco	los	12.4xc	All	All	All
Operating System	Cisco	los	12.4xd	All	All	All
Operating System	Cisco	los	12.2ex	All	All	All
Operating System	Cisco	los	12.2ira	All	All	All
Operating System	Cisco	los	12.2irb	All	All	All

Operating System	Cisco	ios	12.2irc	All	All	All
Operating System	Cisco	ios	12.2sb	All	All	All
Operating System	Cisco	ios	12.2sca	All	All	All
Operating System	Cisco	ios	12.2scb	All	All	All
Operating System	Cisco	ios	12.2se	All	All	All
Operating System	Cisco	ios	12.2sra	All	All	All
Operating System	Cisco	ios	12.2srb	All	All	All
Operating System	Cisco	ios	12.2src	All	All	All
Operating System	Cisco	ios	12.2srd	All	All	All
Operating System	Cisco	ios	12.2sxh	All	All	All
Operating System	Cisco	ios	12.2sxi	All	All	All
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	12.3t	All	All	All
Operating System	Cisco	ios	12.3xl	All	All	All
Operating System	Cisco	ios	12.3xr	All	All	All
Operating System	Cisco	ios	12.3xs	All	All	All
Operating System	Cisco	ios	12.3xx	All	All	All
Operating System	Cisco	ios	12.3ya	All	All	All
Operating System	Cisco	ios	12.3yd	All	All	All
Operating System	Cisco	ios	12.3yf	All	All	All

Operating System	Cisco	ios	12.3yg	All	All	All
Operating System	Cisco	ios	12.3yh	All	All	All
Operating System	Cisco	ios	12.3yi	All	All	All
Operating System	Cisco	ios	12.3yq	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	12.3yu	All	All	All
Operating System	Cisco	ios	12.3yx	All	All	All
Operating System	Cisco	ios	12.3yz	All	All	All
Operating System	Cisco	ios	12.4	All	All	All
Operating System	Cisco	ios	12.4t	All	All	All
Operating System	Cisco	ios	12.4xb	All	All	All
Operating System	Cisco	ios	12.4xc	All	All	All
Operating System	Cisco	ios	12.4xd	All	All	All
cpe:2.3:o:cisco:ios:12.2ex:*****:						
cpe:2.3:o:cisco:ios:12.2ira:*****:						
cpe:2.3:o:cisco:ios:12.2irb:*****:						
cpe:2.3:o:cisco:ios:12.2irc:*****:						
cpe:2.3:o:cisco:ios:12.2sb:*****:						
cpe:2.3:o:cisco:ios:12.2sca:*****:						
cpe:2.3:o:cisco:ios:12.2scb:*****:						
cpe:2.3:o:cisco:ios:12.2se:*****:						
cpe:2.3:o:cisco:ios:12.2sra:*****:						
cpe:2.3:o:cisco:ios:12.2srb:*****:						
cpe:2.3:o:cisco:ios:12.2src:*****:						

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

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

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

```
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:12.3t:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.3x|*:~::~:*~:::
```

```
cpe:2.3:o:cisco:ios:12.3xr:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.3xs:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.3x:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.3ya:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.3yd:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.3yf:*:*:*:*:*:
```

```
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:12.3yq:*:*:*:*:*:
```

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

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

```
cpe:2.3:o:cisco:ios:12.3yu:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.3yx:*.:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.3yz:*.:.:.:.:.:.:
```

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

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

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

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

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

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

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

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

```
cpe:2.3:o:cisco:ios:12.2irc:~::~::~:
```

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

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

```
cpe:2.3:o:cisco:ios:12.2scb:*.:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.2se:*.:*:*:*:*:*:
```

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

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

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

```
cpe:2.3:o:cisco:ios:12.2srd:*.:*:*:*:*:*:
```

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

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

```
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:12.3t:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:12.3x|*:~::~:*~::*
```

```
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:12.3yf:*:*:*:*:*:
```

```
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:12.3yq:*****:
cpe:2.3:o:cisco:ios:12.3ys:*****:
cpe:2.3:o:cisco:ios:12.3yt:*****:
cpe:2.3:o:cisco:ios:12.3yu:*****:
cpe:2.3:o:cisco:ios:12.3yx:*****:
cpe:2.3:o:cisco:ios:12.3yz:*****:
cpe:2.3:o:cisco:ios:12.4:*****:
cpe:2.3:o:cisco:ios:12.4t:*****:
cpe:2.3:o:cisco:ios:12.4xb:*****:
cpe:2.3:o:cisco:ios:12.4xc:*****:
cpe:2.3:o:cisco:ios:12.4xd:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)