

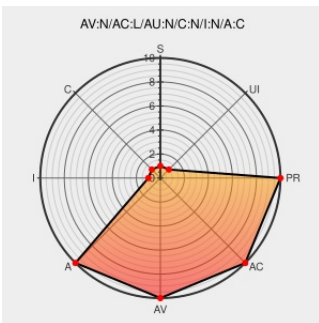


CVE-2010-2836

Published on: 09/23/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:09 PM UTC

CVE-2010-2836

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

Certain versions of **ios** from **Cisco** contain the following vulnerability:

Memory leak in the SSL VPN feature in Cisco IOS 12.4, 15.0, and 15.1, when HTTP port redirection is enabled, allows remote attackers to cause a denial of service (memory consumption) by improperly disconnecting SSL sessions, leading to connections that remain in the CLOSE-WAIT state, aka Bug ID CSCtg21685.

CVE-2010-2836 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 SSL VPN Vulnerability - Cisco Systems

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

[CISCO 20100922 Cisco IOS SSL VPN 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)

Known/Annotated Configurations (OS-E V2.0)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios	12.4	All	All	All
Operating System	Cisco	ios	12.4gc	All	All	All
Operating System	Cisco	ios	12.4mda	All	All	All
Operating System	Cisco	ios	12.4mr	All	All	All
Operating System	Cisco	ios	12.4mra	All	All	All
Operating System	Cisco	ios	12.4sw	All	All	All
Operating System	Cisco	ios	12.4xa	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
Operating System	Cisco	ios	12.4xe	All	All	All
Operating System	Cisco	ios	12.4xf	All	All	All
Operating System	Cisco	ios	12.4xg	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	12.4xl	All	All	All
Operating System	Cisco	ios	12.4xm	All	All	All
Operating System	Cisco	ios	12.4xn	All	All	All
Operating System	Cisco	ios	12.4xp	All	All	All
Operating System	Cisco	ios	12.4xt	All	All	All
Operating System	Cisco	ios	12.4xv	All	All	All
Operating System	Cisco	ios	12.4xw	All	All	All

Operating System	Cisco	los	12.4xy	All	All	All
Operating System	Cisco	los	12.4xz	All	All	All
Operating System	Cisco	los	12.4ya	All	All	All
Operating System	Cisco	los	12.4yb	All	All	All
Operating System	Cisco	los	12.4yd	All	All	All
Operating System	Cisco	los	15.0m	All	All	All
Operating System	Cisco	los	15.0xa	All	All	All
Operating System	Cisco	los	15.1(1)xb1	All	All	All
Operating System	Cisco	los	15.1t	All	All	All
Operating System	Cisco	los	15.1\ (1\)xb1	All	All	All
Operating System	Cisco	los	12.4	All	All	All
Operating System	Cisco	los	12.4gc	All	All	All
Operating System	Cisco	los	12.4mda	All	All	All
Operating System	Cisco	los	12.4mr	All	All	All
Operating System	Cisco	los	12.4mra	All	All	All
Operating System	Cisco	los	12.4sw	All	All	All
Operating System	Cisco	los	12.4xa	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	12.4xe	All	All	All
Operating System	Cisco	los	12.4xf	All	All	All
Operating System	Cisco	los	12.4xg	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	12.4xl	All	All	All
Operating System	Cisco	ios	12.4xm	All	All	All
Operating System	Cisco	ios	12.4xn	All	All	All
Operating System	Cisco	ios	12.4xp	All	All	All
Operating System	Cisco	ios	12.4xt	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	12.4ya	All	All	All
Operating System	Cisco	ios	12.4yb	All	All	All
Operating System	Cisco	ios	12.4yd	All	All	All
Operating System	Cisco	ios	15.0m	All	All	All
Operating System	Cisco	ios	15.0xa	All	All	All
Operating System	Cisco	ios	15.1t	All	All	All
Operating System	Cisco	ios	15.1\{1\}xb1	All	All	All
cpe:2.3:o:cisco:ios:12.4:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.4gc:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.4mda:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.4mr:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.4mra:*:*:*:*:*:						
cpe:2.3:o:cisco:ios:12.4sw:*:*:*:*:*:						

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

```
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:12.4xe:*:*:*:*:*:
```

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

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

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

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

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

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

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

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

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

```
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:12.4ya:*.~::~:
```

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

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

```
cpe:2.3:o:cisco:ios:15.0m:*.:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.0xa:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1(1)xb1:::*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:cisco:ios:15.1t:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1(1)xb1:::~
```

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

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

-----0 0-----10 4mode.*.*.*.*.*.

```
cpe:2.3:0:cisco:ios:12.4mda:::~::~:
```

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

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

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

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

```
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:12.4xe:*:*:*:*:*:
```

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

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

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

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

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

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

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

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

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

```
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:12.4ya:*:*:*:*:*:
```

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

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

```
cpe:2.3:o:cisco:ios:15.0m:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.0xa:*.:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1t:*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:ios:15.1(1\)\xb1:~::~::~:
```

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](#)