



rces

olkit

Search Bugs

My Notifications

[< Back to Previous Page](#)

CSCtx38806 Bug Details

IOS SSL VPN fails to connect after microsoft security update KB2585542

Symptoms: SSL VPN users lose connectivity as soon as Windows machine gets updated with security update KB2585542. This affects Cisco AnyConnect clients and may also affect IE browsers.

This can affect any browser that has the BEAST SSL vulnerability fix, which uses SSL fragmentation (record-splitting). (Chrome v16.0.912 browser is affected for clientless WebVPN on Windows and MAC.)

The problem affects Firefox also (version 10.0.1) displaying the following message:

"The page isn't redirecting properly"

Conditions: This symptom is observed on Cisco IOS that is acting as head end for SSL VPN connections.

Workaround: Any of the following workarounds will work:

- 1) Use the clientless portal to start the client. This only works in some versions of Cisco IOS.
- 2) Uninstall the update.
- 3) Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:

```
w ebvpn gateway gateway name
ssl encryption rc4-md5
```

- 4) Use AC 2.5.3046 or 3.0.3054.
- 5) Use older versions of Firefox (9.0.1).

Further Problem Description: For AnyConnect users, the following user error message is seen:

"Connection attempt has failed due to server communication errors. Please retry the connection"

The AnyConnect event log will show the following error message snippet:

```
Function: Connectfrc::connect
Invoked Function: Connectfrc::handleRedirects
Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED
```

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Status

Fixed
(Resolved)

Severity

2 - severe

Last Modified

In Last 3 Days

Product

Cisco IOS
software

Technology

1st Found-In

15.0(1)M
15.1(1)T
15.1(2)T
15.1(3)T
15.1(4)M
15.2(1)T
15.2(2)T
[Know n](#)
[Affected](#)
[Versions](#)

Fixed-In

15.1(3)T4
15.1(4)M3.8
15.2(3.1)T
15.0(1)M8
15.2(2)T0.12
15.1(1)T4.4
12.4(24)T7
15.2(1)T2.2
15.1(2)T4.3
15.1(4)XB8
15.1(2)T5
15.1(3)T3.1
15.2(3)T0.2
15.2(3)T1
15.2(3.30)PIP

Component(s)

ssl-vpn

Regression

Y

Interpreting This Bug

Bug Toolkit provides access to the latest raw bug data so you have the earliest possible knowledge of bugs that may affect your network, avoiding un-necessary downtime or inconvenience. Because you are viewing a live database, sometimes the information provided is not yet complete or adequately documented. To help you interpret this bug data, we suggest the following:

- The status of this bug is **Resolved**. The problem described in the bug report is "fixed-in" all release versions targeted to be fixed and all changes have been successfully tested. Normally, the assigned engineer moves a bug report into this state.
- The fix is contained in the next major release following any or all of the versions listed in the "fixed-in" section.
- The "fixed-in" version may not be available for download yet until all the other bugs targeted to be fixed for that major

release are processed. No release date information is available to Bug Toolkit. Please check the software download section frequently to look for a new version.

- Sometimes the bug details, when available, contain the "fixed-in" version information or link to the upgrade or patch.
- Any "workaround" listed in the bug details section is generally provided as a way to circumvent the bug until the code fix has been completed; often in lieu of downgrading to a non-affected version of code.
- Check for a release later than these listed versions in software download center.
- The "fixed-in" version may not be available for download yet until all the other bugs targeted to be fixed for that major release are processed. No release date information is available to Bug Toolkit. Please check the software download section frequently to look for a new version.
- Always check the software release notes before performing any upgrade to understand new functionality and open bugs not yet fixed.
- In certain rare circumstances, we are unable to fix the bug in all versions in which it is found. The bug will still have a 'fixed' status. Please open a service request with the Technical Assistance Center if you are being impacted by a bug in this condition.
- Regression bugs are usually caused during the fix of another bug and the bug is usually introduced to the code at this version. Older versions are not usually affected by regression bugs.
- This bug has a **Severe** severity level 2 designation. Important functions are unusable but the router's other functions and the rest of the network is operating normally.
- This bug may not affect the IOS-running product you selected but is provided as a possible match. Remember IOS bugs are rarely platform-specific but all platforms do not necessarily allow the use of all the features included in a given IOS release. For this reason, Bug Toolkit could display a bug that obviously doesn't affect your platform.
- This bug may not affect your version but was returned as a likely possibility since it was introduced but not fixed within the version range you are searching (See Known Affected Versions link.)
- Severity levels are designated by the engineering teams working on the bug. Severity is not an indication of customer priority which is another value used by engineering teams to determine overall customer impact.
- Bug documentation often assumes intermediate to advanced troubleshooting and diagnosis knowledge. Novice users are encouraged to seek fully documented support documents and/or utilize other support options available.

Please use [Bug Search Tool](#) to save bugs, manage notifications. Please visit [help page](#) for more details.

Please rate your overall experience with Bug Toolkit (include the search experience, setting notifications for bugs, ease of getting to bug information, etc).

- Excellent
- Good
- Average
- Fair
- Poor

Were the bug details provided in your search results effective in solving your problem?

- Yes
- No
- Just browsing

Please provide us with suggestions to improve the Bug Content Details or the Bug Toolkit experience:

You may contact me regarding my feedback

Full Name:

Email:

[Contacts](#) | [Feedback](#) | [Help](#) | [Site Map](#)

© 1992-2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)