AnyConnect Hostscan Signature Verification Error on Linux

TAC   **Document ID: 116040**

Contributed by Atri Basu and Jay Young, Cisco TAC Engineers.
Oct 01, 2013

Contents

Introduction

This document describes how to resolve a Cisco AnyConnect Secure Mobility Client connection error if you deploy Hostscan on Linux.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco AnyConnect
- Cisco Secure Desktop (CSD)
- Linux

Components Used

The information in this document affects Linux users who run CSD Hostscan.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problem

When a Linux user runs Cisco Anyconnect in conjunction with CSD Hostscan, an error message appears that indicates the *Posture Assessment Failed* with a *Hostscan Initialize error*:
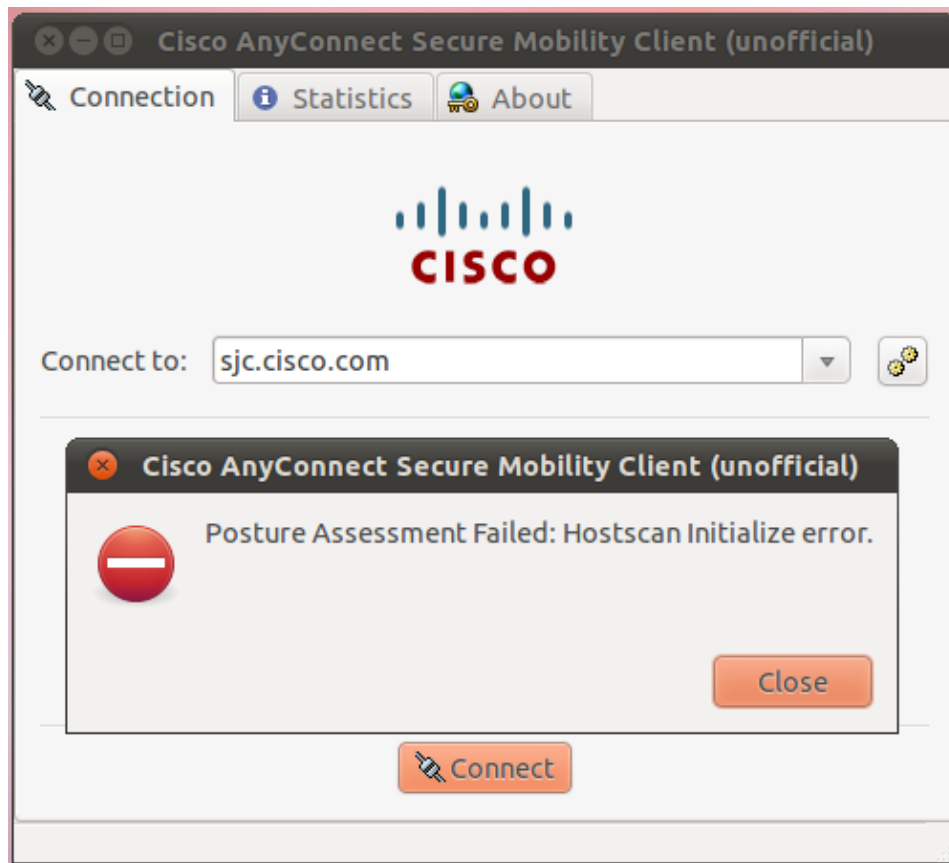
In the *libcsd.log* file, an error message indicates that the certificate used in order to sign the CSD Hostscan binary has expired:

```
[Thu Feb 07 18:52:15.774 2013][libcsd][all][csd_init]
  hello
[Thu Feb 07 18:52:15.774 2013][libcsd][all][csd_init]
  libcsd.so version 3.1.02040
[Thu Feb 07 18:52:15.774 2013][libcsd][debug]
  [hs_transport_init] initialization
[Thu Feb 07 18:52:15.774 2013][libcsd][debug]
  [hs_file_verify_with_killdate] verifying file
  signature: file = [/opt/cisco/anyconnect/lib/libaccurl.so.4.2.0],
  signer = [Cisco Systems, Inc.], type = [2]
[Thu Feb 07 18:52:15.963 2013][libcsd][error][verify_cb]
  Error 10, certificate has expired
[Thu Feb 07 18:52:15.963 2013][libcsd][error][verify_cert]
  Certificate is not trusted
[Thu Feb 07 18:52:15.964 2013][libcsd][error]
  [hs_file_verify_with_killdate] unable to verify
  the certificate trust.
[Thu Feb 07 18:52:15.964 2013][libcsd][error][hs_dl_load_global]
  file signature invalid, not
  loading library (/opt/cisco/anyconnect/lib/libaccurl.so.4.2.0).
```

Note: Mac and Windows users are not affected by this issue. This is because the Mac and Windows client code verifies that the certificate used for signing is *valid at the time of code signing*, whereas the Linux client code checks if the certificate used for signing is *currently valid*.

Solution

Since the problem is caused by the date on which the certificate was signed, you can change the system clock in order to allow the user to connect; however, this is not a fix.

Cisco bug ID CSCue49663 (registered customers only) was filed in order to resolve this problem. In order to get the fix, upgrade to AnyConnect Version 3.1.02043, or upgrade only the Hostscan Engine package to Version 3.0.11046, as shown here:

```
webvpn
enable outside
csd hostscan image disk0:/hostscan_3.1.02043-k9.pkg
csd enable
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1 regex "Windows NT"
anyconnect image disk0:/anyconnect-macosx-i386-3.1.02040-k9.pkg 2 regex "Mac OS"
anyconnect image disk0:/anyconnect-linux-3.1.02043-k9.pkg* 3 regex "Linux"
```

Note: These inks connect to the correct versions of the software downloads (registered customers only).

Updated: Oct 01, 2013   Document ID: 116040