

12/22/2016

To Whom It May Concern,

Acumen Security verified that the following software faithfully embeds a FIPS 140 validated cryptographic module,

- AnyConnect Desktop, version 4.3

The AnyConnect Desktop software is known to operate on the following Operating Systems:

- Windows 7,
- Windows 8,
- Windows 8.1,
- Windows 10,
- Mac OSX 10.8,
- Mac OSX 10.9,
- Mac OSX 10.10,
- Mac OSX 10.11,
- RHEL 6,
- RHEL 7,
- Ubuntu 12.04,
- Ubuntu 14.04.

As part of this review, the software was tested on the following platforms:

- Windows 10

During the course of the review, Acumen Security confirmed that the following cryptographic module is incorporated into the product,

- Cisco FIPS Object Module, version 6.0, FIPS 140-2 certificate # 2505

Acumen Security confirmed that the software leverages the embedded cryptographic module to provide cryptographic services for **TLS** and **IKEv2/IPsec**, including:

- All session establishment associated with the following cryptographic services:
- All underlying cryptographic algorithms supporting the key derivation functions for following cryptographic services:
- All bulk encryption associated with the following services:

Each of the above referenced services can be configured in a manner that restricts algorithm selection to only FIPS 140-2 approved algorithms.

Additionally, Acumen Security confirmed that the above referenced embedded cryptographic module is initialized in a manner consistent with the instructions provided in the non-proprietary Security Policy. Details of the verification may be obtained from Cisco Systems, Inc. at the request of interested parties. This letter represents the independent opinions of Acumen Security and does not imply endorsement of the product by the CMVP or any other parties.

Sincerely,



Ashit Vora  
Laboratory Director