ACUMEN
S E C U R I T Y

2400 Research Blvd, Suite 395
Rockville, MD 20850
tel: +1 (703) 375-9820
info@acumensecurity.net
www.acumensecurity.net

July 22, 2019

To Whom It May Concern:

Acumen Security verified that the following products faithfully embed a FIPS 140-2 validated cryptographic module,

- Cisco WSA v11.8

The software is known to operate on the following platforms

- Web Security Appliances: S690, S690X, S695, S695F, S680, S390, S395, S190, S195, S100v, S300v, S600v
- Virtual products running on UCS C-series running on ESXi 6.0 and 6.5

During the course of the review, Acumen Security confirmed that the following FIPS 140-2 cryptographic module is incorporated into the product,

- Cisco FIPS Object Module (FOM) (Software Version 6.2) – Cert # 2984

Acumen Security confirmed that the following features leverage the embedded cryptographic module to provide cryptographic services for *TLS(HTTPS)*, *SSHv2 and SCP*

1. Session establishment supporting each service,
2. All underlying cryptographic algorithms supporting each services' key derivation functions,
3. Hashing for each service,
4. Symmetric encryption for each service.

Additionally, Acumen Security confirmed that the above referenced 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
Acumen Security