April 4, 2018

To whom it may concern,

Cygnacom’s Cryptographic Equipment Assessment Laboratory (CEAL) has verified that the following Illumio, Inc. (Illumio) products faithfully incorporate the use of the cryptographic functions provided by the FIPS 140-2 validated modules detailed below:

- Policy Compute Engine (PCE) version 18.1-FIPS
- Virtual Enforcement Node (VEN) for Linux version 18.1
- Virtual Enforcement Node (VEN) for Windows version 18.1

The cryptographic operations performed apply to data in transit. The specific uses of the FIPS 140-2 validated modules with the Illumio products are specified as follows:

- Policy Compute Engine (PCE) version 18.1-FIPS: Illumio affirms that the Red Hat Enterprise Linux OpenSSL Cryptographic Module and Google Inc. BoringCrypto are built, initialized and operated in a manner that is FIPS 140-2 compliant, as per the associated security policies and applicable CMVP caveat.

The associated security policies and CMVP caveat can be found here: [https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3016.pdf](https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3016.pdf)


- Virtual Enforcement Node (VEN) for Linux version 18.1: Illumio affirms that the OpenSSL FIPS Object Module SE and Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module are built, initialized and operated in a manner that is FIPS 140-2 compliant, as per the associated security policies and applicable CMVP caveat.

The associated security policies and CMVP caveat can be found here: [https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2393.pdf](https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2393.pdf)


• Illumio Virtual Enforcement Node (VEN) for Windows version 18.1: Illumio affirms that the Microsoft Corporation Kernel Mode Cryptographic Primitives Library (cng.sys) is initialized and operated in a manner that is FIPS 140-2 compliant, as per the associated security policies and applicable CMVP caveat.

The associated security policies and CMVP caveat can be found here:


Sincerely,

Nithya Rachamadugu
CEAL Director
Cryptographic Equipment Assessment Laboratory (CEAL)
Cygnacom Solutions
April 4, 2018

To whom it may concern,

Cygnacom's Cryptographic Equipment Assessment Laboratory (CEAL) has verified that the "Policy Compute Engine (PCE) version 18.1-FIPS" of Illumio, Inc. (Illumio) faithfully incorporates the cryptographic functions represented in the following cryptographic modules:

<table>
<thead>
<tr>
<th>Module Name</th>
<th>FIPS 140-2 Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux OpenSSL Cryptographic Module (Software Version: 5.0)</td>
<td>Cert. #3016</td>
</tr>
<tr>
<td>Google Inc, BoringCrypto (Software Version: 24e5886c0edfc409c8083d10f9f1120111efd6f5)</td>
<td>Cert. #2964</td>
</tr>
</tbody>
</table>

**Red Hat Enterprise Linux 7.4**

Illumio affirms that the Red Hat Enterprise Linux OpenSSL Cryptographic Module (Software Version: 5.0) and the Google Inc. BoringCrypto (Software Version: 24e5886c0edfc409c8083d10f9f1120111efd6f5) used by the Illumio Policy Compute Engine (PCE) version 18.1-FIPS are built, initialized and operated in a manner that is FIPS 140-2 compliant on the Red Hat Enterprise Linux 7.4 operating system using the associated FIPS 140-2 security policies (URL’s below) as a reference.


Sincerely,

Nithya Rachamadugu
CEAL Director
Cryptographic Equipment Assessment Laboratory (CEAL) 
Cygnacom Solutions
April 4, 2018

To whom it may concern,

Cygnacom's Cryptographic Equipment Assessment Laboratory (CEAL) has verified that the "Virtual Enforcement Node (VEN) for Linux version 18.1" of Illumio, Inc. (Illumio) faithfully incorporates the cryptographic functions represented in the following cryptographic modules:

<table>
<thead>
<tr>
<th>Module Name</th>
<th>FIPS 140-2 Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenSSL FIPS Object Module SE (Software Version: 2.0.9, 2.0.10, 2.0.11, 2.0.12, 2.0.13, 2.0.14, 2.0.15 or 2.0.16)</td>
<td>Cert. #2398</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v4.0 (Software Version: 4.0)</td>
<td>Cert. #2742</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module (Software Version: 5.0)</td>
<td>Cert. #3145</td>
</tr>
</tbody>
</table>

**Red Hat Enterprise Linux 7.1**

Illumio affirms that the OpenSSL FIPS Object Module SE (Software Version: 2.0.9, 2.0.10, 2.0.11, 2.0.12, 2.0.13, 2.0.14, 2.0.15 or 2.0.16) and Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v4.0 (Software Version: 4.0) used by the Illumio Virtual Enforcement Node (VEN) version 18.1 are built, initialized and operated in a manner that is FIPS 140-2 compliant on the Red Hat Enterprise Linux 7.1 operating system using the associated FIPS 140-2 security policies as a reference.


**Red Hat Enterprise Linux 7.4**

Illumio affirms that the OpenSSL FIPS Object Module SE (Software Version: 2.0.9, 2.0.10, 2.0.11, 2.0.12, 2.0.13, 2.0.14, 2.0.15 or 2.0.16) and Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module (Software Version: 5.0) used by the Illumio Virtual Enforcement Node (VEN) version 18.1 are built, initialized and operated in a manner that is FIPS 140-2 compliant on the Red Hat Enterprise Linux 7.4 operating system using the associated FIPS 140-2 security policies as a reference.


Sincerely,

Nithya Rachamadugu
CEAL Director
Cryptographic Equipment Assessment Laboratory (CEAL)
Cygnacom Solutions
April 4, 2016

To whom it may concern,

Cygnacom’s Cryptographic Equipment Assessment Laboratory (CEAL) has verified that the "Virtual Enforcement Node (VEN) for Windows version 18.1" of Illumio, Inc. (Illumio) faithfully incorporates the cryptographic functions represented in the following cryptographic modules:

<table>
<thead>
<tr>
<th>Module Name</th>
<th>FIPS 140-2 Certificate</th>
</tr>
</thead>
</table>

**Microsoft Windows Server 2012 R2**

Illumio affirms that the Microsoft Corporation Kernel Mode Cryptographic Primitives Library (cng.sys) (Software Version: 6.3.9600 and 6.3.9600.17042) used by the Illumio Virtual Enforcement Node (VEN) version 18.1 is initialized and operated in a manner that is FIPS 140-2 compliant on the Microsoft Windows Server 2012 R2 operating system using the associated FIPS 140-2 security policy as a reference.


**Microsoft Windows Server 2016**

Illumio affirms that the Microsoft Corporation Kernel Mode Cryptographic Primitives Library (cng.sys) (Software Version: 10.0.14393) used by the Illumio Virtual Enforcement Node (VEN) version 18.1 is initialized and operated in a manner that is FIPS 140-2 compliant on the Microsoft Windows Server 2016 operating system using the associated FIPS 140-2 security policy as a reference.
Sincerely,

Nithya Rachamadugu
CEAL Director
Cryptographic Equipment Assessment Laboratory (CEAL)
Cygnacom Solutions