# FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America


The Canadian Centre for Cyber Security

**July 2022**

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: TIMOTHY HALL Digitally signed by TIMOTHY HALL Date: 2022.08.03 09:39:27 -04'00'

Dated:

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: King, Lyall Digitally signed by King, Lyall DN: C=CA, O=GC, OU=CSE-CST, CN="King, Lyall" Reason: I am approving this document Location: your signing location here Date: 2022.08.03 08:37:02-04'00' Foxit PDF Editor Version: 11.2.1

Dated:

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

| Certificate Number | Validation / Posting Date | Module Name(s) | Vendor Name | Version Information |
|---|---|---|---|---|
| 4260 | 07/06/2022 | Druva FIPS Cryptographic Module | Druva Inc. | Software Version: 2.2 |
| 4261 | 07/08/2022 | HSSD_V6 Series | Huawei Technologies Co., Ltd. | Hardware Version: HSSD-D7294DL1T9E, HSSD-D7294DL3T8E, HSSD-D7294DL7T6E; Firmware Version: 1063 |
| 4262 | 07/08/2022 | SonicWall Network Security Virtual Appliances | SonicWall, Inc. | Firmware Version: SonicOSX 7.0 |
| 4263 | 07/13/2022 | NITROXIII CNN35XX-NFBE HSM Family | Marvell | Hardware Version: P/Ns CNL3560P-NFBE-G, CNL3560P-NFBE-2.0-G, CNL3560P-NFBE-3.0-G, CNL3560B-NFBE-2.0-G, CNL3560B-NFBE-3.0-G, CNL3560-NFBE-G, CNL3560-NFBE-2.0-G, CNL3560-NFBE-3.0-G, CNL3560A-NFBE-3.0-G, CNL3560C-NFBE-3.0-G, CNL3560D-NFBE-3.0-G, CNL3560E-NFBE-3.0-G, CNL3560F-NFBE-3.0-G, CNL3530-NFBE-G, CNL3530-NFBE-2.0-G, CNL3530-NFBE-3.0-G, CNL3530B-NFBE-2.0-G, CNL3530B-NFBE-3.0-G, CNL3530A-NFBE-3.0-G, CNL3530C-NFBE-3.0-G, CNL3530D-NFBE-3.0-G, CNL3530E-NFBE-3.0-G, CNL3530F-NFBE-3.0-G, CNL3510-NFBE-G, CNL3510-NFBE-2.0-G, CNL3510-NFBE-3.0-G, CNL3510P-NFBE-G, CNL3510P-NFBE-2.0-G, CNL3510P-NFBE-3.0-G, CNL3510A-NFBE-3.0-G, CNL3510C-NFBE-3.0-G, CNL3510D-NFBE-3.0-G, CNL3510E-NFBE-3.0-G, CNL3510F-NFBE-3.0-G, CNN3560P-NFBE-G, CNN3560P-NFBE-2.0-G, CNN3560P-NFBE-3.0-G, CNN3560-NFBE-G, CNN3560-NFBE-2.0-G, CNN3560-NFBE-3.0-G, CNN3560A-NFBE-3.0-G, CNN3560C-NFBE-3.0-G, CNN3560D-NFBE-3.0-G, CNN3560E-NFBE-3.0-G, CNN3560F-NFBE-3.0-G, CNN3530-NFBE-G, CNN3530-NFBE-2.0-G, CNN3530-NFBE-3.0-G, CNN3530A-NFBE-3.0-G, CNN3530C-NFBE-3.0-G, CNN3530D-NFBE-3.0-G, CNN3530E-NFBE-3.0-G, CNN3530F-NFBE-3.0-G, CNN3510-NFBE-G, CNN3510-NFBE-2.0-G, CNN3510-NFBE-3.0-G, CNN3510A-NFBE-3.0-G, CNN3510C-NFBE-3.0-G, CNN3510D-NFBE-3.0-G, CNN3510E-NFBE-3.0-G, CNN3510F-NFBE-3.0-G, CNN3510LP-NFBE-2.0-G, CNN3510LP-NFBE-3.0-G, CNN3510LPB-NFBE-2.0-G, CNN3510LPB-NFBE-3.0-G, CNN3510LPA-NFBE-3.0-G, CNN3510LPC-NFBE-3.0-G, CNN3510LPD-NFBE-3.0-G, CNN3510LPE-NFBE-3.0-G, CNN3510LPF-NFBE-3.0-G, CNN3505LP-NFBE-2.0-G, CNN3505LP-NFBE-3.0-G, CNN3505LPA-NFBE-3.0-G,CNN3505LPC-NFBE-3.0-G, CNN3505LPD-NFBE-3.0-G, CNN3505LPE-NFBE-3.0-G and CNN3505LPF-NFBE-3.0-G; Firmware Version: CNN35XX-NFBE-FW-1.1 build 02 and CNN35XX-NFBE-FW-1.1 build 05 |
| 4264 | 07/15/2022 | Check Point Cryptographic Library | Check Point Software Technologies Ltd. | Firmware Version: 1.1 |
| 4265 | 07/17/2022 | Inline Crypto Engine (ICE) | Google, LLC | Hardware Version: 1.0 |
| 4266 | 07/18/2022 | Oracle Linux 7 Libreswan Cryptographic Module | Oracle Corporation | Software Version: R7-7.8.0 |

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

| Certificate Number | Validation / Posting Date | Module Name(s) | Vendor Name | Version Information |
|---|---|---|---|---|
| 4267 | 07/18/2022 | Security Builder® FIPS Module | BlackBerry Limited | Software Version: 6.5.0 |
| 4268 | 07/18/2022 | Ultrastar® DC SN840 NVMe™ PCIe 3.0 Self Encrypting Drive | Western Digital Technologies, Inc. | Hardware Version: P/Ns WUS4C6416DSP3X5, WUS4BA119DSP3X5, WUS4C6432DSP3X5, WUS4BA138DSP3X5, WUS4C6464DSP3X5, WUS4BA176DSP3X5 and WUS4BA1A1DSP3X5; Firmware Version: R2210400 and R2EF0003 |
| 4269 | 07/18/2022 | Ultrastar® DC HC550 TCG Opal Self-Encrypting Drive and Ultrastar® DC HC650 TCG Opal Self-Encrypting Drive | Western Digital Corporation | Hardware Version: P/Ns WUH721818AL4206 [2],WUH721816ALN6L6 [2], WSH722020AL4206 [1]; Firmware Version: R463 [1] and R670 [2] |
| 4270 | 07/18/2022 | Ultrastar® DC SN540 NVMe™ PCIe 3.0 Self-Encrypting Drive and Ultrastar® DC ZN540 NVMe™ PCIe 3.0 Self-Encrypting Drive | Western Digital Corporation | Hardware Version: P/Ns WUS4B7619DSP305 [1], WUS4B7638DSP305 [1], WUS4B7676DSP305 [1], WUS4B7696DSP305 [1], WZS4C8T1TDSP305 [2], WZS4C8T2TDSP305 [2], WZS4C8T4TDSP305 [2], and WZS4C8T8TDSP305 [2]; Firmware Version: R611000Q [1] and R6Z10022 [2] |
| 4271 | 07/18/2022 | Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module | Red Hat(R), Inc. | Software Version: rhel8.20210325 |
| 4272 | 07/18/2022 | Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module | Red Hat(R), Inc. | Software Version: rhel8.20210401 |
| 4273 | 07/25/2022 | Microsoft Azure Networking Adapter Kernel | Microsoft Corporation | Software Version: 1.0; Hardware Version: BCM58732 |
| 4274 | 07/26/2022 | Instant-On Networks (ION) devices ION 1000, ION 2000, ION 3000, ION 7000, and ION 9000 | Palo Alto Networks, Inc. | Hardware Version: ION 1000, ION 2000, ION 3000, ION 7000, and ION 9000; Firmware Version: 5.5.1 |