BLUVECTOR®
A COMCAST COMPANY

Cortex - FIPS 140-2 Level 1 Validated Certificate Numbers

BluVector Cortex Release 3.7.0 is FIPS 140-2 Level 1 Compliant. This document provides list of FIPS 140-2 validated cryptographic modules implemented in the release and links to certificates

FIPS 140-2 Level 1 Validation

BluVector Cortex Release 3.7.0 is FIPS 140-2 Level Compliant. This document provides information on the FIPS 140 validated cryptographic modules in the Sensor and Central Manager.

The FIPS 140-2 process was completed in January 2020 in conjunction with Acumen Security, who are accredited by the U.S. Federal Government National Institute of Standards and Technology (NIST) for Cryptographic and Security Testing.

List of Cryptographic Modules Included in the Product

- Red Hat Enterprise Linux OpenSSL Cryptographic Module, Version 5.0 or 6.0, FIPS 140-2 certificate #3016
- Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module, Version 6.0, FIPS 140-2 certificate #3292
- Red Hat Enterprise Linux OpenSSH Server Cryptographic Module, Version 5.0 or 6.0, FIPS 140-2 certificate #3063
- Red Hat Enterprise Linux NSS Cryptographic Module, Version 6.0, FIPS 140- 2 certificate #3270
- Red Hat Enterprise Linux GnuTLS Cryptographic Module, Version 5.0, FIPS 140-2 certificate #3012

Links to Certificates of Cryptographic Modules Included in the Product

Certificate #3016 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3016

Certificate #3292 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3292

Certificate #3063 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3063

Certificate #3270 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3270

Certificate #3012 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3012

FIPS 140-2 Level 1

About BluVector, A Comcast Company

As a leader in network security, BluVector is empowering security teams to get answers about real threats, allowing businesses and governments to operate with greater confidence that data and systems are protected.

BLUVECTOR MLE

BluVector MLE is a patented supervised Machine Learning Engine that was developed within the defense and intelligence community to accurately detect zero-day and polymorphic malware in real time. Unlike unsupervised machine learning, which is leveraged by most security vendors today, BluVector MLE algorithms were pretrained to immediately identify malicious content embedded within common file formats like Office documents, archives, executables, .pdf, and system updates. The result: 99.1%+ detection accuracy upon installation.

BLUVECTOR SCE

BluVector SCE is the security market's first analytic specifically designed to detect fileless malware as it traverses the network. By emulating how the malware will behave when it is executed, the Speculative Code Execution engine determines, at line speed, what an input can do if executed and to what extent these behaviors might initiate a security breach. By covering all potential execution chains and focusing on malicious capacity rather than malicious behavior, the analytic technology vastly reduces the number of execution environments and the quantity of analytic results that must be investigated.

BLUVECTOR®
A COMCAST COMPANY

www.bluvector.io 571.565.2100