ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Guardtime Federal's Black Lantern® BL300 Series and BL400 BLKSI.2.2.2-FIPS

Maintenance Report Number: CCEVS-VR-VID11287-2024

Date of Activity: 25 June 2024

References:

Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

Collaborative Protection Profile for Network Devices Version 2.2e, 23 March 2020 [NDcPP]

Impact Analysis Report for Guardtime Federal Black Lantern® BL300 and BL400 Series with BLKSI.2.2.1-FIPS, Version 1.0, April 29, 2024

Guardtime Federal Black Lantern® BL300 Series and BL400 with BLKSI.2.2.2-FIPS Security Target, Version 1.1, 29 April 2024

Assurance Continuity Maintenance Report:

Guardtime Federal submitted an Impact Analysis Report (IAR) and Assurance Continuity Maintenance package to the CCEVS for approval in April 2024. The IAR is intended to satisfy the requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consists of the Security Target (ST) and the Impact Analysis Report (IAR). The ST was updated to reflect the new version of the TOE.

Documentation Updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Guardtime Federal Black Lantern® BL300 Series	See references above. Document is updated to reflect the new firmware

and BL400 with BLKSI.2.2.1-FIPS Security Target, Version 1.1, 29 April 2024	version. Section 1.1 was updated to provide the correct current name and version of the ST and the TOE. Sections 1.6 and 1.8 was updated to provide the correct firmware version of the TOE. The version of the ST is now 1.1 and the date April 29, 2024.
Design Documentation: See Security Target	No changes have been made to the Security Target beyond revisions to identify the new version of the TOE.
Guidance Documentation: **None**	No changes required
Lifecycle: None	No changes required
Testing: None	Guardtime Federal has performed regression testing on the evaluated product.
Vulnerability Assessment: None	The public search was performed on 10 January 2024 and again on 24 June 2024. No public vulnerabilities exist within the product. See analysis of results below.

Changes to the TOE:

Guardtime Federal made networking improvements to the TOE firmware to introduce networking improvements. The TOE firmware was updated to BLKSI.2.2.2-FIPS, summarized below.

Major Changes

None.

Minor Changes

BLKSI.2.2.2-FIPS Changes	
Change	**Analysis**

Upon network error or disruption, the BL will attempt to recover existing network settings, specifically gateway and static routes to re-establish good network status when the network has been restored.	Minor: This is non-security functionality that is not touched in any way by the CC testing or SFRs.
Static routes can be configured regardless of the actual route available on the network.	Minor: This is non-security functionality that is not touched in any way by the CC testing or SFRs.

Regression Testing:
Guardtime Federal initiated this maintenance action to improve networking functionality present in the TOE. Guardtime Federal applied the networking changes into the TOE and developed and executed testing activities specific to the networking changes. Guardtime Federal also performed regression testing of the entire TOE to ensure that the TOE continued to perform as expected at the time of the original evaluation.

Equivalency:

The security functionality of the BLKSI.2.2.2-FIPS firmware update remains the same as the prior evaluated version. The hardware platforms are unchanged from the original evaluation version.

NIST CAVP Certificates:

The same cryptographic modules are used in BLKSI.2.2.1-FIPS and in BLKSI.2.2.2-FIPS. The CAVP certificate numbers referenced during the BLKSI.2.2.1-FIPS evaluation have not changed.

Vulnerability Analysis

For all third-party dependencies, there were no updates in release version BLKSI.2.2.2-FIPS. A search for known publicly disclosed vulnerabilities was performed against the National Vulnerability database on January 10, 2024 and again on June 24, 2024. The search terms used were:

- BL300-B2
- BL300-C2
- BL400-A1
- NXP T4240r2 QorIQ
- Power Architecture
- BLKSI.2.2.1-FIPS
- Cryptographic Support Library (CSL) Direct
- Green Hills

Of the results found for those search terms, none were identified as applicable or in direct use within the TOE's source code base. There are no publicly-disclosed cybersecurity vulnerabilities applicable (in use) to the changed TOE. Therefore, no additional mitigation is required to the changed TOE.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found the changes to be minor and did not affect the evaluated security functionality. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.