ASSURANCE CONTINUITY MAINTENANCE REPORT for Black Box Secure KVM/Matrix and KM Switch

Maintenance Update for: Black Box Secure KVM/Matrix and KM Switch

Maintenance Report Number: CCEVS-VR-VID10893-2019

Date of Activity: 21 June 2019

References:

- Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 3, September 12, 2016
- Impact Analysis Report for Black Box Secure KVM/Matrix and KM Switch (IAR), Version 1.0, May 20, 2019
- Protection Profile for Peripheral Sharing Switch Version 3.0, February 13, 2015 (PP_PSS_v3.0)
- Validation Report for Black Box Secure KVM/Matrix and KM Switch, Report Number CCEVS-VR-10893-2018, dated August 3, 2018, Version 1.0

Documentation report as being updated:

- Security Target – Black Box Secure KVM/Matrix and KM Switch Security Target, Version 1.14, May 10, 2018. Updated to: Black Box Secure KVM/Matrix and KM Switch Security Target, Version 1.15, May 20, 2019
- Administrative Guide- Black Box Secure KVM Administration and Security Management Tool Guide (KVM/Matrix and KM), Version 1.1, May 10, 2018. Updated to: Black Box Secure KVM Administration and Security Management Tool Guide (KVM/Matrix and KM), Version 1.2, May 20, 2019.

Assurance Continuity Maintenance Report:

Leidos Common Criteria Testing Laboratory, on behalf of Black Box Corporation, submitted an

Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 24 May 2019. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 3, September 12, 2016. In accordance with those requirements, the IAR describes the changes made to the certified Target of Evaluation (TOE), the evidence that was updated as a result of those changes, and the security impact of those changes.

Introduction:

The Black Box Secure KVM/Matrix and KM Switch (hereafter referred to as the TOE) was evaluated by Leidos Common Criteria Testing Laboratory and issued a NIAP CCEVS certificate on August 3, 2018. The product met the requirements specified by the NIAP-approved protection profile for PP_PSS_v3.0.

The purpose of this document is to summarize and represent CCEVS’ analysis and findings regarding Assurance Maintenance Continuity as the CC documentation has been updated.

Summary Description:

The TOE includes a “multi-head display mode” option where cursor-controlled switching cannot be engaged until the user has first pressed the center mouse button (scroll wheel) twice. In the original evaluation, “multi-head display mode” is described as a voluntary option within the administrative guidance. In order ensure the T.UNINTENDED_SWITCHING threat from the PP is properly addressed, this Assurance Maintenance Continuity was completed to enforce “multi-head display mode” as mandatory for the CC evaluated configuration for KM models, or when KVM models are configured in KM mode. A new vulnerability scan was also performed.

Changes to TOE:

There have been no changes to the product or development environment.

The evaluated TOE includes models with Keyboard-Mouse (KM) switching functionality only; i.e. no switching of video display. Most KVM models of the TOE can also be set to a “KM mode” that disables the video ports and causes the TOE to operate as if it was a KM device only. In these cases, the selected computer can be switched by one of two methods:

- Push-button toggles on the TOE hardware to switch to the desired computer
- Moving the mouse cursor to the edge of the screen on the selected computer to switch to the ‘next computer over’ (note that since the TOE does not have any displays connected to it while in this configuration, the conditions for switching are detected by the (x,y) coordinates of the mouse)

The TOE includes a “multi-head display mode” option where cursor-controlled switching cannot be engaged until the user has first pressed the center mouse button (scroll wheel) twice. In the original evaluation, “multi-head display mode” is described as a voluntary option within the administrative guidance. In order ensure the T.UNINTENDED_SWITCHING threat from the PP is properly addressed, this Assurance Maintenance Continuity was completed to enforce “multi-head display mode” as mandatory for the CC evaluated configuration for KM models, or when KVM models are configured in KM mode.

The Security Target (ST) and Administrative Guidance have been updated to instruct administrators/users that “multi-head display mode” switching is required for the evaluated configuration for KM models of the TOE, or when a KVM model is configured in KM mode.

Affected Developer Evidence:

CC Evidence	Evidence Change Summary
Original Security Target: Black Box Secure KVM/Matrix and KM Switch Security Target, Version 1.14, May 10, 2018	**Maintained Security Target:** Black Box Secure KVM/Matrix and KM Switch Security Target, Version 1.15, May 20, 2019 Changes in the maintained ST are: • Updated identification of ST • Updated product description in introduction/TSS
Common Criteria Administrative Guide: Black Box Secure KVM Administration and Security Management Tool Guide (KVM/Matrix and KM), Version 1.1, May 10, 2018	**Maintained Common Criteria Administrative Guide:** Black Box Secure KVM Administration and Security Management Tool Guide (KVM/Matrix and KM), Version 1.2, May 20, 2019 Changes in the maintained Guidance are: • Updated KM mode configuration instructions to state that “multi-head display mode” must also be enabled once KM mode has been set.

Regression Testing:

No regression testing was performed as no changes to the product were required.

Vulnerability Analysis:

A search of national sites was conducted for vulnerabilities related to the TOE. The public search was updated on May 20, 2019. No public vulnerabilities exist in the product.

Conclusion:

CCEVS reviewed the documentation changes and concur the changes are minor and that certificate maintenance is the correct path for assurance continuity as defined in NIAP Publication #6. In addition, the evaluator reported having conducted an updated vulnerability search that located no new applicable vulnerabilities requiring mitigation. Therefore, CCEVS agrees that the original assurance is maintained for the product.