CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

The Boeing Company Boeing Black with Hardware ID v.6.0.2 and PureSecure v1.3

Maintenance Report Number: CCEVS-VR-VID10615-2015a

Date of Activity: 20 March 2015

References:

Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 2, September 8, 2008

Common Criteria Document CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements” Version 1, February 2004

The Boeing Company Boeing Black (MDFPP20) Security Target, Version 1.0, February 20, 2015

Boeing PureSecure Administrator Guidance for PureSecure v.1.2.6, February 4, 2015

Evaluation Technical Report for Boeing Black (MDFPP20), Version 0.1, January 30, 2015

Impact Analysis Report for The Boeing Company Boeing Black, Revision 1.0, March 2, 2015

Boeing PureSecure 1.3.0 Software Test Report, February 19, 2015 (Proprietary)

Affected Evidence:

Boeing PureSecure Administrator Guidance for PureSecure v.1.2.6, February 4, 2015

The Boeing Company Boeing Black (MDFPP20) Security Target, Version 1.0, February 20, 2015.

Updated Developer Evidence:

The Boeing Company Boeing Black (MDFPP20) Security Target, Version 1.1, March 2, 2015

Boeing PureSecure Administrator Guidance v1.0.6 for PureSecure v1.3, March 2, 2015

Assurance Continuity Maintenance Report:

Gossamer Security Solutions CCTL on behalf of The Boeing Company, submitted an Impact Analysis Report to CCEVS for approval. 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 2, September 8, 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence that was updated as a result of those changes, and the security impact of those changes.

Changes to TOE:

The TOE has been updated in the following areas:

The TOE has been revised from the evaluated Boeing Black with Hardware ID v6.0.2 and PureSecure v1.2.6 to Boeing Black with Hardware ID v6.0.2 and PureSecure v1.3

1. Support for Ethernet has been added. Software has been added to support a USB-Ethernet adapter and a management function to enable and disable the support has been added.

2. The ability to install and load accessory module drivers has been disabled. In the previous evaluation, Boeing stipulated that the administrator disable USB Debugging to prevent the user from installing and loading of accessory module drivers. The new software disables installing and loading accessory module drivers altogether, so the USB Debugging restriction is no longer needed.

3. One of the MDM API functions had an incorrect argument type and was causing admin apps to crash. This code bug has been corrected.

Vendor Conclusion:

The Boeing Black was revised to add one feature and fix two bugs. These changes are primarily related to Ethernet support and mandatory policy restrictions and as indicated above none are related to the security claims in the evaluated ST. A limited regression test was also performed to ensure these new changes did not negatively impact existing functionality.

The evaluation evidence consists of the Security Target, administrative guidance, design documents, life cycle documents, and test evidence. The Security Target was revised to reflect the new version. The guidance has been updated to reflect the new version, identify the Ethernet support, and remove the USB Debugging restriction, but otherwise all guidance includes the content evaluated in the previous versions.

Note that Boeing continually tracks bugs, vulnerabilities, and other defects reported in the public domain and at the time of this report there are no known outstanding security-related vulnerabilities in the TOE.

Validation Team Conclusion:

In an examination of the bug fixes implemented, the validators found that the fixes were unrelated to the original security functional requirements in the Security Target. The added feature can be considered a minor change; and the fixes applied to the TOE software resulted in functionality that is consistent with the certified functionality. To support this claim, the vendor developed and performed their standard regression test cases to ensure the changes did not negatively impact existing functionality. NIAP has reviewed the vendors regression testing and considers it sufficient.

The validation team reviewed the changes and concur the changes are minor and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.