CCEVS Approved Assurance Continuity Maintenance Report

Assurance Continuity Maintenance Report for
Microsoft Windows 8.1, Microsoft Windows RT 8.1, Microsoft Windows Server 2012 R2

Maintenance Update of Microsoft Windows 8.1, Microsoft Windows RT 8.1, Microsoft Windows Server 2012 R2

Maintenance Report Number: CCEVS-VR-VID10540-2015

Conformance: Software Full disk Encryption Protection Profile, Version 1.1, March 31, 2014

Date of Activity: 11 July 2015

References: Common Criteria Evaluation and Validation Scheme - Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0 , September 8, 2008

Microsoft Windows 8.1, Microsoft Windows Server 2012 R2 Full Disk Encryption Impact Analysis Report, Version 1.0, May 8, 2015

Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption Security Target, Version 1.0, April 3, 2014

I. Introduction

Microsoft has submitted an Impact Analysis Report (IAR) for the Microsoft Windows 8.1 and Microsoft Windows Server 2012 R2 Full Disk Encryption capability to CCEVS for approval. The TOE is part of the Windows operating system that implements Full Disk Encryption functionality, and thus the TOE includes the Microsoft Windows 8 operating system, the Microsoft Windows Server 2012 operating system, and supporting hardware. Microsoft refers to the Full Disk Encryption capability as “BitLocker”. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme - Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0 , September 8, 2008 and Scheme Policy Letter #22. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes, and the security impact of the changes.

II. Changes to the TOE

There are two broad changes made to the product. The first change is to specify the “.1” release as the evaluated configuration. This entails updating the TOE Software Identification to the following products:

- Microsoft Windows 8.1 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 8.1 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2012 R2 Standard Edition
- Microsoft Windows Server 2012 R2 Datacenter Edition

The second change is to add updated hardware configurations to those currently approved:

- Microsoft Surface Pro 3, Intel Core i7, 64-bit (added)
- Microsoft Surface 3**,** Intel Atom Z8700, 64-bit (added)

III. Analysis and Testing

While changes to the base Windows product are numerous in moving from 8.0 to 8.1, the functionality that pertains to the Full Disk Encryption requirements was not affected by any of these changes. No administrative nor programmatic interfaces change as a result of the update. The developer submitted this version of the OS to NIST, and the CAVP certificates associated with the evaluated configuration have been updated:

Cryptographic Operation	Standard	Windows 8 Evaluation Method	Windows 8.1 Evaluation Method
Encryption/Decryption	FIPS 197 AES For ECB, CBC, CFB8, CCM, and GCM modes	NIST CAVP #2197, #2216	NIST CAVP #2848, #2832, #2853
Digital signature	FIPS 186-3 rDSA for Windows 8 FIPS 186-4 rDSA for Windows 8.1	NIST CAVP #1134, #1133	NIST CAVP #1487, #1493, #1494, #1519
Digital signature	FIPS 186-3 ECDSA for Windows 8 FIPS 186-4 ECDSA for Windows 8.1	NIST CAVP #341	NIST CAVP #505
Hashing	FIPS 180-3	NIST CAVP #1903	NIST CAVP #2373, #2396
Random number generation	NIST SP 800-90	NIST CAVP #259 for Dual_EC_DRBG NIST CAVP #258 for CTR_DRBG	NIST CAVP #489 for CTR_DRBG

The hardware includes new versions of the Surface devices, which do not differ from the previously-evaluated Surface Pro device in a manner that impacts the requirements of the Full Disk Encryption PP. In addition to Microsoft's corporate regression-testing activities, Microsoft also re-performed the tests that were done as part of the original evaluation. Finally, a search was performed in the public domain for any new potential vulnerabilities that may have been identified since the evaluation completed. No potential vulnerabilities were found that might affect any of the security claims. The CCTL performed no additional testing.

IV. Conclusion

While the number of changes between Windows 8.0 and 8.1 are numerous, the IAR categorized those changes and adequately justified the minor impact to the requirements against which the original configuration was tested. The hardware additions are updates to previously-evaluated models, with no significant differences between the old and new models in terms of the impact due to the requirements.

Therefore, the validators have determined that the changes to the previously evaluated version of this product with respect to the Full Disk Encryption SFRs are minor, and were determined to be acceptable.