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-VID10529-2015

Conformance: Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.1, December 30, 2012

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 RT 8.1, Microsoft Windows Server 2012 R2 VPN Client Impact Analysis Report, Version 1.0, May 8, 2015

Microsoft Windows 8, Microsoft Windows RT 8, Microsoft Windows Server 2012 VPN Client Security Target, Version 1.0, January 23, 2014

I. Introduction

Microsoft has submitted an Impact Analysis Report (IAR) for the Microsoft Windows 8.1, Microsoft Windows RT 8.1, and Microsoft Windows Server 2012 R2 VPN Client to CCEVS for approval. The TOE is part of the Windows operating system that implements VPN client functionality, and thus the TOE includes the Microsoft Windows 8 operating system, the Microsoft Windows RT operating system, the Microsoft Windows Server 2012 operating system, and supporting hardware. There are two mechanisms covered that invoke the IPsec VPN client: the Remote Access Service (RAS) VPN interface and the (raw) IPsec interface. 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 Edition (32-bit and 64-bit versions)
- 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 RT 8.1
- Microsoft Windows Server 2012 R2 Standard Edition
- Microsoft Windows Server 2012 R2 Datacenter Edition

The second change is to update the evaluated hardware platforms to remove hardware no longer available, and replace it with updated hardware configurations:

- Microsoft Surface 3
- Microsoft Surface Pro 3
- ASUS VivoTab RT
- Dell XPS 10
- Dell OptiPlex 755, 3.0 GHz Intel Core 2 Duo E8400, 64-bit

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 VPN client 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 DSA for Windows 8 FIPS 186-4 DSA for Windows 8.1	NIST CAVP #687	NIST CAVP #855
Digital signature	FIPS 186-3 rDSA for Windows 8 FIPS 186-4 DSA 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	SHA-256, SHA-384, and SHA-512	NIST CAVP #1903	NIST CAVP #2373, #2396
Key Agreement	EC DH	NIST CAVP #36	NIST CAVP #47
Keyed-Hash Message Authentication Code	HMAC	NIST CAVP #1345	NIST CAVP #1773
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 updated versions of the Surface devices, which do not differ from the previously-evaluated devices in a manner that impacts the requirements of the VPN Client 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 VPN Client SFRs are minor, and were determined to be acceptable.