ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Microsoft Windows 10 IPsec VPN Client (VPNPP14)

Microsoft Windows 10 IPsec VPN Client (VPNPP14)

Maintenance Report Number: CCEVS-VR-VID10753-2017a

Date of Activity: 27 November 2017

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;

Impact Analysis Report for Microsoft Windows 10 Anniversary Update IPsec VPN Client, Version 1.0, September 08, 2017

Documentation reported as being updated:

- Microsoft Windows 10 IPsec VPN Client Security Target, version 0.05, 2017/10/05
- Microsoft Windows 10 (Creators Update) IPsec VPN Client Operational Guidance, version 0.8, 2017/08/01

Assurance Continuity Maintenance Report:

Leidos, on behalf of The Microsoft Corporation, submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 8 September 2017. 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 2.0. 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.

The IAR identifies the changes to the TOE, which include the addition of the Dell 5285 as part of the updated evaluated TOE Hardware Identification, new and updated content and IT pro features in Windows 10, version 1703 (Creators Update), patches for software updates for vulnerabilities, as well as other non-security claim relevant changes.

The addition of the Dell 5285 requires testing to verify that the results of the VPN Client evaluation are consistent for this device. Additional VPN client testing was also performed for the Creators Update to verify that all test results are consistent with those of the original evaluation and evaluated configuration. A summary of this testing including detailed information on which tests were run on which platforms can be found in the Windows 10 (Creators Update) VPN IAR Testing

Excel workbook. New certificate numbers for the appropriate NIST CAVP standards in the evaluation using the new Windows 10 (Creators Update) Operating System were added. NIAP has verified these NIAP CAVP certificates and subsequent documentation as adequate.

In addition, patches for software updates for vulnerabilities are prepared as required by various policies and VPN requirements.

Non-security claim relevant changes were also made to the Windows 10 Anniversary Update and Creators Update; these changes were deemed outside the scope of the VPN evaluation. These include multiple enhancements to Windows 10 (Creators Update) such as the addition of the Windows Configuration Designer, Azure Active Directory join in bulk feature, Windows Spotlight features, Start and taskbar layout, Cortana at work, and other deployment, update, and management features. For these, the evaluated configuration is unaffected. In the case of the pause update feature for Windows Update for Business, it is provided as an option to give the administrator more flexibility but does not affect the core update services as part of the Windows 10 Anniversary Update evaluation (and thus assurance is maintained).

The addition of the Dell 5285, which required additional testing that was performed, as well as software updates for vulnerabilities listed above constitute the only security-based changes to the TOE.

The evaluation evidence consists of the Security Target, Operational Guidance (AGD), Vulnerability Analysis, Impact Analysis Report (IAR), and IAR Testing. The Security Target, Operational Guidance, and IAR include the model numbers affected, which are the Surface Pro 4, Surface Book, and newly evaluated Dell 5285.

Note that Microsoft 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.

Changes to TOE:

The specific device in question consists of the Surface Pro 4, Surface Book, and newly evaluated Dell 5285. Except for the addition of the Dell 5285 and CAVP certificates for the Windows 10 Creators Update, the device has not changed in security functionality; only the descriptions of the validated configuration have changed. The changes and effects based on ST and AGD modifications are summarized below.

1. The addition of the Dell 5285 requires testing to verify that the results of the VPN Client evaluation are consistent for this device.

Security Consideration	Assessment
The following hardware platforms and components are included in the original evaluated configuration: • Surface Book	This is a security-relevant modification to the TOE because a new product was included (the Dell 5285).

• Surface Pro 4 The following hardware platforms and components are included in the updated evaluated configuration: • Surface Book • Surface Pro 4 • Dell 5285 <u>Later in the IAR:</u> "Testing on for both Windows 10 (Anniversary Update) and Windows 10 (Creators Update) produced consistent test results. See the Windows 10 (Creators Update) VPN IAR Testing.xlsx spreadsheet for detailed information on which tests were run on which platforms. The green boxes in the spreadsheet indicate passing test results. Changes to Certificate Numbers."	The impact is that testing must be verified for the Dell 5285. Microsoft has provided a summary testing document, Windows10 (Creators Update) VPN IAR Testing.xlsx, which shows the platforms being tested. Microsoft states in the IAR that testing "produced consistent test results." Because a new platform is utilized, testing also includes ensuring that updated CAVP certificate numbers are sufficient. NIAP has assessed the CAVP certificates listed in both the ST and IAR and have found them to be sufficient. The result is a PASS, and the net security effect of the changes is minimal. Original assurance is maintained.

2. General Security Updates

Security Consideration	Assessment
Finally, a search was performed in the public domain for any new potential vulnerability that may have been identified since the evaluation completed which is described in "Windows 10 (Creators Update) VPN Client Assurance Maintenance: Vulnerability Analysis". No potential vulnerabilities were found that might affect any of the security claims.	This is consistent with all applicable NIAP policies and VPN requirements related to vulnerabilities. Original assurance is maintained.

3. Enhancements to Windows 10 (Creators Update)

Security Consideration	Assessment
Windows Configuration Designer Previously known as Windows Imaging and Configuration Designer (ICD), the tool for creating provisioning packages is renamed Windows Configuration Designer. The new Windows Configuration Designer is available in Windows Store as an app. To run Windows Configuration	This is not security relevant because it was outside the scope of the Windows 10 (Anniversary Update) VPN Client evaluation and Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same.

Designer on earlier versions of Windows, you can still install Windows Configuration Designer from the Windows Assessment and Deployment Kit (ADK). Windows Configuration Designer in Windows 10, version 1703, includes several new wizards to make it easier to create provisioning packages.	
Azure Active Directory join in bulk Using the new wizards in Windows Configuration Designer, you can create provisioning packages to enroll devices in Azure Active Directory. Azure AD join in bulk is available in the desktop, mobile, kiosk, and Surface Hub wizards.	This is not security relevant because Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same.
Windows Spotlight New Group Policy and mobile device management (MDM) settings are added to help you configure Windows Spotlight user experiences.	This is not security relevant because it was outside the scope of the Windows 10 (Anniversary Update) VPN Client evaluation and Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same.
Start and taskbar layout Enterprises have been able to apply customized Start and taskbar layouts to devices running Windows 10 Enterprise and Education. In Windows 10, version 1703, customized Start and taskbar layout can also be applied to Windows 10 Pro. Previously, the customized taskbar could only be deployed using Group Policy or provisioning packages. Windows 10, version 1703, adds support for customized taskbars to MDM.	This is not security relevant because it was outside the scope of the Windows 10 (Anniversary Update) VPN Client evaluation and Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same.
Cortana at work Cortana is Microsoft's personal digital assistant, who helps busy people get things done, even while at work. Cortana has powerful configuration options, specifically optimized for your business. By signing in with an Azure Active Directory (Azure AD) account, your employees can give	This is not security relevant because Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same.

Cortana access to their enterprise/work identity, while getting all the functionality Cortana provides to them outside of work.	Moreover, pre-installed apps are provided by device manufacturers, OS developers, and mobile carriers. They provide capabilities outside of scope and do not provide security functionality mandated by the VPN PP. Because AVA_VAN.1 limits the scope of vulnerability search activities, the original assurance of the product is not affected.
MBR2GPT.EXE MBR2GPT.EXE is a new command-line tool available in Windows 10 version 1703 and later versions. MBR2GPT converts a disk from Master Boot Record (MBR) to GUID Partition Table (GPT) partition style without modifying or deleting data on the disk. The tool is designed to be run from a Windows Preinstallation Environment (Windows PE) command prompt, but can also be run from the full Windows 10 operating system (OS).	This is not security relevant because Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same. Moreover, pre-installed apps are provided by device manufacturers, OS developers, and mobile carriers. They provide capabilities outside of scope and do not provide security functionality mandated by the VPN PP. Because AVA_VAN.1 limits the scope of vulnerability search activities, the original assurance of the product is not affected.
Windows Defender Advanced Threat Protection New features in Windows Defender Advanced Threat Protection (ATP) for Windows 10, version 1703.	This is not security relevant because it was outside the scope of the Windows 10 (Anniversary Update) VPN Client evaluation and Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same. Moreover, pre-installed apps are provided by device manufacturers, OS developers, and mobile carriers. They provide capabilities outside of scope and do not provide security functionality mandated by the VPN PP.

	Because AVA_VAN.1 limits the scope of vulnerability search activities, the original assurance of the product is not affected.
Group Policy Security Options The security setting Interactive logon: Display user information when the session is locked has been updated to work in conjunction with the Privacy setting in Settings > Accounts > Sign-in options. A new security policy setting Interactive logon: Don't display username at sign-in has been introduced in Windows 10 version 1703. This security policy setting determines whether the username is displayed during sign in. It works in conjunction with the Privacy setting in Settings > Accounts > Sign-in options. The setting only affects the Other user tile.	This is not security relevant because it was outside the scope of the Windows 10 (Anniversary Update) VPN Client evaluation and Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same.
Windows Hello for Business You can now reset a forgotten PIN without deleting company managed data or apps on devices managed by Microsoft Intune. For Windows desktops, users are able to reset a forgotten PIN through Settings > Accounts > Sign-in options.	This is not security relevant because it was outside the scope of the Windows 10 (Anniversary Update) VPN Client evaluation and Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same.
Windows Information Protection (WIP) and Azure Active Directory (Azure AD) Microsoft Intune helps you create and deploy your Windows Information Protection (WIP) policy, including letting you choose your allowed apps, your WIP-protection level, and how to find enterprise data on the network. For more info, see Create a Windows Information Protection (WIP) policy using Microsoft Intune and Associate and deploy your Windows Information Protection (WIP) and VPN policies by using Microsoft Intune. You can also now collect your audit event logs by using the Reporting configuration service provider (CSP) or the Windows Event Forwarding (for Windows desktop domain-joined devices).	This is not security relevant because it was outside the scope of the Windows 10 (Anniversary Update) VPN Client evaluation and Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same.

Windows Update for Business The pause feature has been changed, and now requires a start date to set up. Users are now able to pause through Settings > Update & security > Windows Update > Advanced options in case a policy has not been configured. We have also increased the pause limit on quality updates to 35 days. You can find more information on pause in Pause Feature Updates and Pause Quality Updates. Windows Update for Business managed devices are now able to defer feature update installation by up to 365 days (it used to be 180 days). In settings, users are able to select their branch readiness level and update deferal periods. See Configure devices for Current Branch (CB) or Current Branch for Business (CBB), Configure when devices receive Feature Updates and Configure when devices receive Quality Updates for details.	This is not security relevant because the changing of the pause update feature does not affect the core update services which were part of the Windows 10 (Anniversary Update) evaluation. The update is still installed however the administrator is now provided with more flexibility. Thus, the claimed and tested VPN functionality remains the same.
Windows Insider for Business We recently added the option to download Windows 10 Insider Preview builds using your corporate credentials in Azure Active Directory (AAD). By enrolling devices in AAD, you increase the visibility of feedback submitted by users in your organization – especially on features that support your specific business needs. For details, see Windows Insider Program for Business.	This is not security relevant because it was outside the scope of the Windows 10 (Anniversary Update) VPN Client evaluation and Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same.
Optimize update delivery With changes delivered in Windows 10, version 1703, Express updates are now fully supported with System Center Configuration Manager, starting with version 1702 of Configuration Manager, as well as with other third-party updating and management products that implement this new functionality. This is in addition to current Express support on Windows Update, Windows Update for Business and WSUS.	This is not security relevant because the update delivery optimizations may be used with Windows 10 (Creators Update) in enterprise scenarios, however these optimizations do not affect the core update services which were part of the Windows 10 (Anniversary Update) evaluation. Thus, the claimed and tested VPN functionality remains the same.

Uninstalled in-box apps no longer automatically reinstall Starting with Windows 10, version 1703, in-box apps that were uninstalled by the user won't automatically reinstall as part of the feature update installation process. Additionally, apps de-provisioned by admins on Windows 10, version 1703 machines will stay de-provisioned after future feature update installations. This will not apply to the update from Windows 10, version 1607 (or earlier) to version 1703.	This is not security relevant because it was outside the scope of the Windows 10 (Anniversary Update) VPN Client evaluation and Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same.
New MDM capabilities Windows 10, version 1703 adds many new configuration service providers (CSPs) that provide new capabilities for managing Windows 10 devices using MDM or provisioning packages. Among other things, these CSPs enable you to configure a few hundred of the most useful Group Policy settings via MDM - see Policy CSP - ADMX-backed policies. Some of the other new CSPs are: The DynamicManagement CSP allows you to manage devices differently depending on location, network, or time. For example, managed devices can have cameras disabled when at a work location, the cellular service can be disabled when outside the country to avoid roaming charges, or the wireless network can be disabled when the device is not within the corporate building or campus. Once configured, these settings will be enforced even if the device can't reach the management server when the location or network changes. The Dynamic Management CSP enables configuration of policies that change how the device is managed in addition to setting the conditions on which the change occurs. The CleanPC CSP allows removal of user-installed and pre-installed applications, with the option to persist user data.	This is not security relevant because although new CSPs and capabilities have been added none of the capabilities used in the Windows 10 (Anniversary Update) VPN Client evaluation are affected. Thus, the claimed and tested VPN functionality remains the same.

The BitLocker CSP is used to manage encryption of PCs and devices. For example, you can require storage card encryption on mobile devices, or require encryption for operating system drives. The NetworkProxy CSP is used to configure a proxy server for ethernet and Wi-Fi connections. The Office CSP enables a Microsoft Office client to be installed on a device via the Office Deployment Tool. For more information, see Configuration options for the Office Deployment Tool. The EnterpriseAppVManagement CSP is used to manage virtual applications in Windows 10 PCs (Enterprise and Education editions) and enables App-V sequenced apps to be streamed to PCs even when managed by MDM.	
Application Virtualization for Windows (App-V) Previous versions of the Microsoft Application Virtualization Sequencer (App-V Sequencer) have required you to manually create your sequencing environment. Windows 10, version 1703 introduces two new PowerShell cmdlets, New-AppVSequencerVM and Connect-AppvSequencerVM, which automatically create your sequencing environment for you, including provisioning your virtual machine. Additionally, the App-V Sequencer has been updated to let you sequence or update multiple apps at the same time, while automatically capturing and storing your customizations as an App-V project template (.appvt) file, and letting you use PowerShell or Group Policy settings to automatically cleanup your unpublished packages after a device restart.	This is not security relevant because it was outside the scope of the Windows 10 (Anniversary Update) VPN Client evaluation and Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed capabilities. Thus, the claimed and tested VPN functionality remains the same.
Windows diagnostic data Microsoft collects Windows diagnostic data to keep Windows up-to-date, secure, and operating properly. It also helps us improve Windows and, for users who have turned on "tailored	This is not security relevant because it was outside the scope of the Windows 10 (Anniversary Update) VPN Client evaluation and Microsoft does not seek to include it in the list of Windows 10 (Creators Update) VPN client's claimed

experiences", can be used to provide relevant tips and recommendations to tailor Microsoft products to the user's needs.	capabilities. Thus, the claimed and tested VPN functionality remains the same.
New Group Policy A number of new policies have been added.	This is not security relevant because although new policies have been added none of the policies used in the in the Windows 10 (Anniversary Update) VPN Client evaluation are affected. Thus, the claimed and tested VPN functionality remains the same.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security. It was determined that the changes affected the documentation as well as CAVP certificates. Because a new device was added, additional testing was required. This testing would be addressed in the IAR Testing Excel workbook where all tests were reperformed and the results were found to be consistent with those of the previous Windows 10 Anniversary Update VPN client evaluation. Since the test results were found to be consistent and the newly acquired CAVP certificates were found to be acceptable by NIAP, the impact upon security was found to be minor.

In addition, the mobile device vendor reported having conducted a vulnerability search update that located no new vulnerabilities up to the end of the previous month as reflected by update newsletters by the platform and mobile device vendors. Further, it was also reported that the vendor did regression testing and that the changes, collectively, had no security impact on the TOE.

Therefore, CCEVS agrees that the original assurance is maintained for the product.