ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Unisys Stealth Solution Release v3.3

Maintenance Update of Unisys Stealth Solution Release v3.0

Maintenance Report Number: CCEVS-VR-VID10716-2017a

Date of Activity: 21 November 2017

References: Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004;

Unisys Stealth Solution Release v3.3 Impact Analysis Report
IAR Version – Version 1.0, 10 October 2017

Documentation Updated: (List all documentation updated)

- **Security Target:** Unisys Stealth Solution Release v3.0 Windows Endpoint Security Target, Version 1.0, 16 June 2016
  - Changes in the maintained ST are:
    - Updated identification of ST
    - Section 1.1 - Updated TOE software version
    - Sections 2.3.1, 2.3.1.1, and 6 - Added Microsoft Windows 10 and Microsoft Windows Server 2016 as compatible endpoint operating systems.
    - Provided a description of the Stealth(aware) functionality in Section 2.2.
    - Replacement of the Stealth Applet with the Stealth Dashboard in Section 2.3.1, 6.5.2, and 6.5.3.
- **Common Criteria Compliance Guide**: Unisys Stealth Solution Common Criteria Evaluation Guidance Document, Release 3.0, June 2016 (8205 5823-000)
  - Changes in the maintained Guidance are:
    - Updated Section 1.2. Common Criteria Evaluation Operating Systems has been updated to include Windows 10 and Windows Server 2016
    - Replaced the reference to the Stealth Applet with the Stealth Dashboard.
    - Updated Section 7. A warning for the administrator not to use the Distribute function to distribute and automatically install updated endpoint software functionality has been added.
    - Updated Section 7.4. Deleted the requirement that Management Server and all Windows endpoints must run Java 7.x.

- **Test**: Evaluation Team Test Report For Unisys Stealth Solution Release v3.0 Windows Endpoint, Version 2.0, June 16, 2016
    - Maintained Test Report (Leidos Proprietary)

Assurance Continuity Maintenance Report:

The vendor for the Unisys Stealth Solution Release v3.3 submitted an Impact Analysis Report (IAR) to CCEVS for approval on October 2017. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 1.0, February 2004. 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.

Changes to TOE:

The changes described in this document constitute all changes made to the Unisys Stealth Solution Release 3.0 Windows Endpoint since the previous Common Criteria evaluation (CCEVS-VR-VID10716-2016). The previous evaluation tested the TOE on the following specific platforms:

- Windows 8 (VID #10520)
- Windows 8.1 (VID #10592)
- Windows Server 2012 R2 (VID #10529).

The Unisys Stealth Solution Release v3.3 Windows Endpoint is supported on the following additional platforms that have all completed Common Criteria evaluations under the Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI). Dossier: 2016-36. The platforms are compliant to the NIAP - Protection Profile for General Purpose Operating Systems, Version: 4.1.

- Microsoft Windows 10
- Microsoft Windows Server 2016

All the evaluated Windows platforms contain the same Windows crypto functions which are accessed thru the same interfaces. No interface calls made by the program required changing to port to the new platforms, and regression testing was performed. The validators judge this change as minor.

The Unisys Stealth Solution Release 3.0 Windows Endpoint software was updated from version 3.0.170.0 to version 3.3.011.0. The updates are summarized below.

1. The Stealth Applet has been replaced with the Stealth Dashboard. The Stealth Applet is part of the TSF as it contributes to satisfaction of FPT_TUD_EXT.1 – it provides the ability to query the current version of the TOE. The validators concur that the relevant SFR is not changed and a change in TOE implementation is at a lower level of granularity than that covered by the PP evaluation. Thus, the change is considered minor.
2. Product updates were made that do not implement SFRs or support SFR satisfaction. These updates are not security relevant because the claimed and tested VPN functionality remains

the same.

- **Capability to distribute updated endpoint packages**
- **New endpoint Configuration Audit Report**
- **Updated Management Server upgrade procedure**
- **Updated endpoint memory requirements and installation prerequisites for Windows, Linux, and AIX endpoints**
- **For Windows endpoints, updated method to disable network adapters**
- **Support for SUSE Linux Enterprise Server 12.x endpoints**
- **Information on minimizing data loss during outages and understanding outage behavior**
- **The process to use RDP with Stealth endpoints has been updated.**
- **Ability to edit filter names and descriptions**

3. The following updates are considered minor because the affected functionality is not covered in the scope of the evaluation.
   - **New ability to optionally update the number of simultaneous downloads when distributing an endpoint package.**
   - **New capability for certificate-based authorization enables certificates to be identified by an object identifier (OID)**
   - **Reorganized installation and configuration procedures to Stealth-enable the Management Server and standalone Authorization Servers earlier in the configuration process**
   - **Enterprise Manager Updates**
   - **Certificate updates**
   - **Updated rekey response and error responses**
   - **Updated Management Server and standalone Authorization Server software requirements**
   - **Updated Management Server procedures**
   - **Changes made to AuthService.config file**
   - **Stealth Ecosystem API (EcoAPI)**
   - **Configure Custom retention period for Configuration Audit Reports**
   - **Unisys Stealth(aware) for new Stealth implementations**
   - **Changes to the AuthService.config file**
   - **Updates to the configuration of Enterprise Manager User Accounts**

4. There are numerous bug fixes that are not relevant for the SFRs, or they were corrections of anomalous behavior to make the behavior agree with the documentation, requirements, and SFRs. As they did not impact the original testing (i.e., below the level of original testing), their correction remains minor.

Regression Testing:

Although only minor changes were made to the functionality of the TOE, extensive regression testing on the new and original hardware platforms demonstrated that the TOE functionality was equivalent. New test results were generated, and were reviewed by Vendor. Testing evidence was submitted with the IAR and was reviewed by the validators.

Conclusion:

The specific changes made to the product do not affect the security claims in the Unisys Stealth Solution Release v3.3 Windows Endpoint Security Target.

This update results in no changes to SFRs, Security Functions, Assumptions or Objectives, Assurance Documents and therefore is a minor change. The security target and the Common Criteria Evaluation Guidance Document are updated to reflect the updates.

Test results were produced and found consistent with the previous test results. Finally, the evaluation security team searched the public domain for any new potential vulnerabilities that may have been identified since the evaluation completed. The search did not identify any new potential vulnerability.

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found it to be **minor**. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.