National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Acronis SCS Cyber Backup 12.5 Hardened Edition Server

Report Number: CCEVS-VR-VID11328-2023
Dated: 10/19/2023
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE:6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Daniel Faigin

The Aerospace Corporation

Farid Ahmed

Anne Gugel

Richard Toren

Johns Hopkins University - Applied Physics Laboratory

Common Criteria Testing Laboratory

Pascal Patin

Allen Sant

Dawn Campbell

Leidos Inc.

Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Acronis SCS Cyber Backup 12.5 Hardened Edition Server (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. In conjunction with this VR, end-users should review the Security Target (ST), which is where specific security claims are made. The ST also describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 9, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in September 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended conformant and meets the assurance requirements of the following document:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5])
- Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019 ([6])

The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found the evaluation demonstrated the product satisfies all the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile, and when installed, configured and operated as described in the evaluated guidance documentation, satisfies all the SFRs specified in the ST ([7]).

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

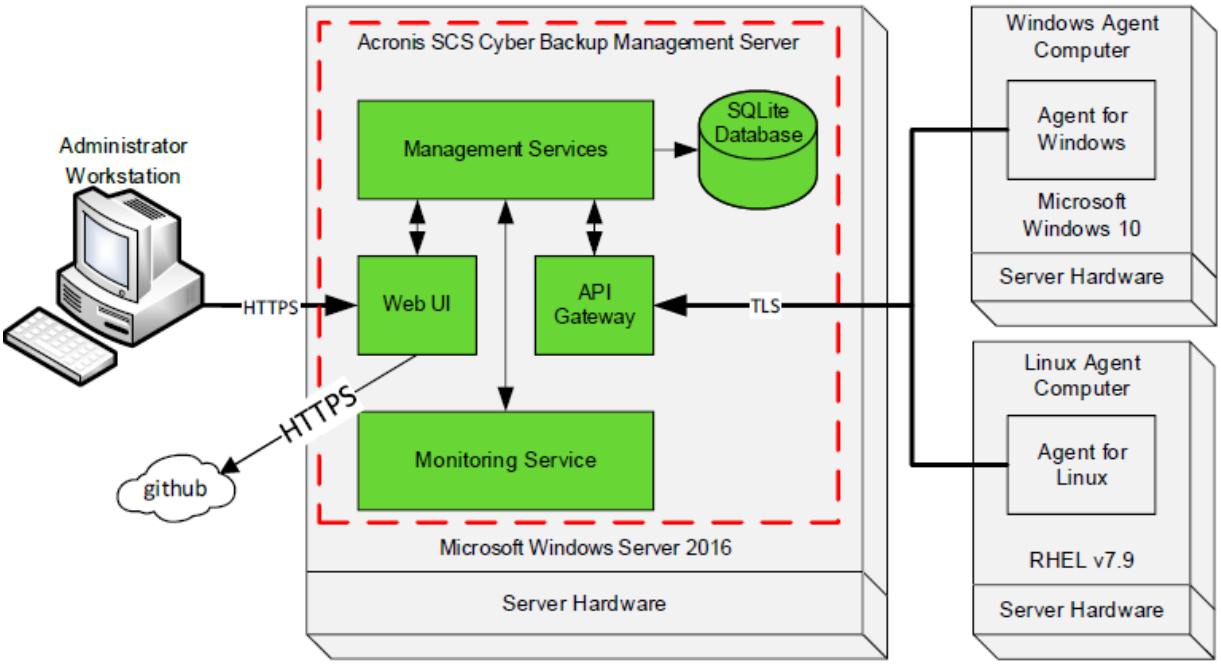
Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Acronis SCS Cyber Backup 12.5 Hardened Edition Server on Windows Server 2016
Security Target	Acronis SCS Cyber Backup 12.5 Hardened Edition Server, Version 0.14, 11 October 2023
Sponsor & Developer	Acronis SCS 1225 W. Washington St., Suite #205, Tempe, AZ 85288
Completion Date	10/19/2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	*Protection Profile for Application Software*, Version 1.4, 7 October 2021 *Functional Package for Transport Layer Security (TLS),* Version 1.1, 1 March 2019
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Allen Sant Kofi Owusu
Validation Personnel	Daniel Faigin Farid Ahmed Anne Gugel Richard Toren

3 TOE Architecture

Note: The following architectural description is based on the description presented in the ST.

The TOE architecture is depicted in the following figure. The TOE is indicated by the dashed red box. The application runs on a Windows Server 2016 as an application.



Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

3.1 Cryptographic Support

The TOE provides cryptographic functions to secure sessions between the administrator workstation connecting via a web browser to the Management Console of the TOE using HTTPS and TLS v1.2. Cryptographic functions are also used to secure communications between the TOE and the Backup Agents in the TOE environment using TLS v1.2. The Acronis SCS Cryptographic Library and Acronis SCS Protocol Library are used to provide the required algorithms and protocols for all cryptographic operations. The TOE also stores its sensitive data in the Windows Data Protection API.

3.2 User Data Protection

The TOE protects sensitive data in non-volatile memory according to the requirements in FCS_STO_EXT.1. The TOE restricts its access to network connectivity provided by the platform's hardware resources. Specifically, it will only use network connectivity for administrative actions over trusted paths to its Management Console and connections via trusted channels from Backup Agents in the TOE environment. The TOE accesses the platform's system logs to store audit information and does not access any other sensitive information repositories.

3.3 Security Management

The TOE does not provide default credentials. It uses the existing administrator accounts on the platform for authentication. The TOE creates a group that is assigned to administrators and used to identify the accounts that have access. The application invokes the mechanisms recommended by the platform vendor for storing and setting configuration options. The TOE and its data are protected against unauthorized access by default file permissions.

3.4 Privacy

The TOE does not transmit Personally Identifiable Information (PII).

3.5 Protection of the TSF

The TOE does not allocate memory with both write and execute permissions and does not write user-modifiable files to directories that contain executable files. The TOE is compiled with the /GS flag to enable stack-based buffer overflow protection and is compatible with the platform's security features. The TOE uses standard platform APIs and includes only the third-party libraries it needs to perform its functionality. The TOE is versioned with SWID tags that comply with the minimum requirements from ISO/IEC 19770-2:2015 and provides the ability to check for updates to the application software.

The TOE is distributed as an additional software package to the platform OS. The TOE is packaged such that its removal results in the deletion of all traces of the application, except for configuration settings, output files, and audit/log events. The TOE does not download, modify, replace or update its own binary code.

3.6 Trusted Path/Channels

The TOE provides trusted paths and trusted channels using its cryptographic functions. The TOE secures administrative communications using HTTPS over TLS v1.2 to its Management Console. The TOE provides trusted communications channels between the TOE and Backup Agents using TLS v1.2.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

4.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following document:
  - *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5])
  - *Functional Package for Transport Layer Security (TLS),* Version 1.1, 1 March 2019 ([6])
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Acronis SCS Cyber Backup 12.5 Hardened Edition Server v12.5 Security Target, Document Version 0.14, October 11, 2023 ([7]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in Section 5 of this VR.

5 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- Acronis Cyber Backup 12.5 SCS Hardened Edition User Guide, Update 4.7 ([8])
- Acronis Cyber Backup 12.5 SCS Hardened Edition Server v12.5 Guidance Documentation Supplement, Version 0.5, October 11, 2023. ([9])

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

6 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- Acronis SCS Cyber Backup 12.5 Management Server Common Criteria Test Report and Procedures, Version 1.1, 11 October, 2023 ([12]).

A non-proprietary description of the tests performed and their results is provided in the following document:

- Assurance Activities Report for Acronis SCS Cyber Backup 12.5 Management Server, Version 1.1, 11 October, 2023 ([11])

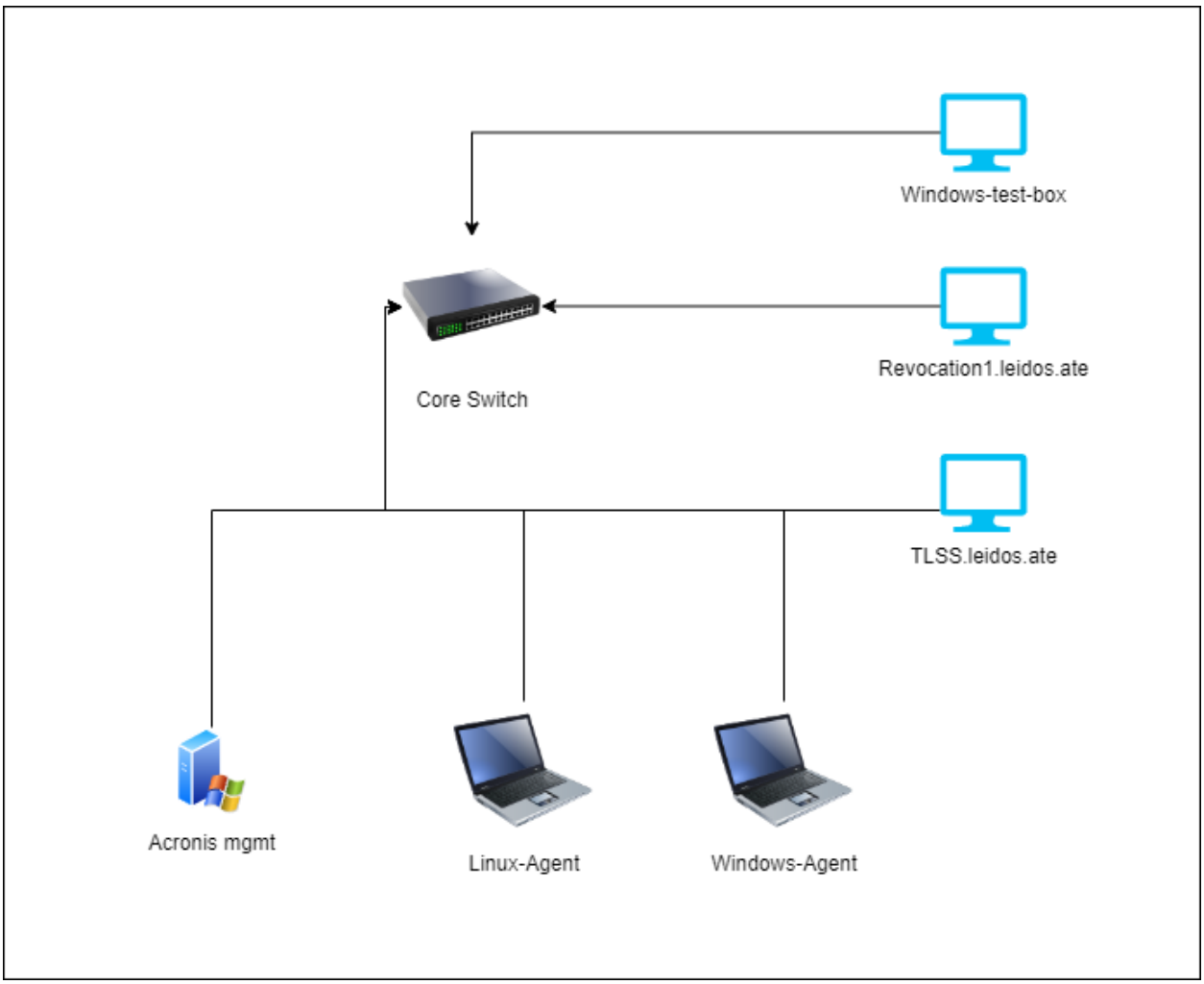
The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the following specification:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021.
- Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019

The evaluation team devised a test plan based on the test activities specified in the PP. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report listed above.

The TOE was tested at Leidos's Columbia, MD location from November 2022 to August 2023. The procedures and results of this testing are available in the test report referenced above.

The following figure identifies the devices used for testing the TOE and describes the test configuration.



The following components were used to create the test configuration:

TOE Platform

- Acronis MGMT
  - Windows Server 2016 Standard

Test Configuration Components

- Linux-Agent
  - Linux host to have the Acronis Agent installed.
- Windows-Agent
  - Windows host to have the Acronis Agent installed.
- Revocation1.leidos.ate
  - Hosts Revocation provider for the Agents.
- TLSS.leidos.ate
  - Ubuntu machine to host test tools.
- Windows-Test-Box
  - Windows 10 machine to access the TOE and host test tools.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the team test plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *Protection Profile for Application Software* and *Functional Package for Transport Layer Security (TLS)* were fulfilled.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is the Acronis SCS Cyber Backup 12.5 Hardened Edition Server v12.5, evaluated on Microsoft Windows Server 2016 OS. The TOE runs on the platform OS as a standalone.

7.2 Excluded Functionality

Only the Features and Functionality specified in the ST were covered by the evaluation. In particular, the following are not part of the evaluated configuration of the TOE:

- Remote and cloud storage locations
- Cloud configuration deployments
- Managing agents for hypervisors, applications, and mobile devices
- Backup functionality

8 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Acronis SCS Cyber Backup 12.5 Management Server ([10]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5]).
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 [(6])

The evaluation determined the TOE satisfies the conformance claims made in the Acronis SCS Cyber Backup 12.5 Hardened Edition Server v12.5 Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the PP listed above.

8.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PP, and security function descriptions that satisfy the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate

the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each test activity and applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA evaluation activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The evaluation team performed a search of the National Vulnerability Database (https://nvd.nist.gov/).

The evaluation team performed searches on 12 April 2023, September 15, and again on October 11, 2023, using the following search terms:

- “Acronis SCS”
- “Cyber Backup”
- “TLS 1.2”

- "Acronis SCS Cryptographic Library"
- "SCS Version-check"
- The identity of each of the third-party libraries listed in Appendix B of the ST.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

8.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed PP. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

9 Validator Comments/Recommendations

All of the validators concerns are adequately captured in Section 4, Assumptions and Clarification of Scope. In particular, the validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 5 to ensure the evaluated configuration is established and maintained.

10 Security Target

The ST for this product's evaluation is *Acronis SCS Cyber Backup 12.5 Hardened Edition Server v12.5 Security Target Document, Version 0.14 October 11, 2023* ([7]).

11 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

[4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] Protection Profile for Application Software, Version 1.4, 07 October 2021.

[6] Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019

[7] Acronis SCS Cyber Backup 12.5 Hardened Edition Server v12.5 Security Target, Document Version 0.14, October 11, 2023

[8] Acronis Cyber Backup 12.5 SCS Hardened Edition User Guide, Update 4.7

[9] Acronis Cyber Backup 12.5 SCS Hardened Edition Server v12.5 Guidance Documentation Supplement, Version 0.5, October 11, 2023.

[10] Evaluation Technical Report for Acronis SCS Cyber Backup 12.5 Management Server, Version 1.1, 11 October 2023.

[11] Assurance Activities Report for Acronis SCS Cyber Backup 12.5 Management Server, Version 1.1, 11 October 2023.

[12] Acronis SCS Cyber Backup 12.5 Management Server Common Criteria Test Report and Procedures, Version 1.1, 11 October 2023.

[13] Acronis SCS Cyber Backup 12.5 Hardened Edition Server v12.5 Vulnerability Assessment, Version 1.2, October 11, 2023.