Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Votiro Secure Data Sanitization Engine Version 7.1

Certification Report
2017/110

16 November 2017
Version 1.0

Amendment Record

Version	Date	Description
0.1	1 November 2017	Internal
0.2	13 November 2017	Internal
1.0	16 November 2017	External

Executive Summary

This report describes the findings of the IT security evaluation of Votiro Secure Data Sanitization Engine version 7.1 against Common Criteria Evaluation Assurance Level 2.

The Target of Evaluation (TOE) is Votiro Secure Data Sanitization Engine version 7.1.

The TOE is a product that is designed to supplement the traditional sandboxing approach for securing files entering a network. It can help detect and prevent 0-day and other advanced threats that are designed to work around the general sandboxing approach. The sanitiser engines implement several proprietary methods of sanitising files such as disrupting malicious code by the introduction of noise or micro changes.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit:** The TOE generates and stores audit files for a variety of auditable events. These events record the identity of the user that caused the event to occur, the date and time, the success/failure of the event and any other pertinent information.
- **User Data Protection:** The TOE implements flow control mechanisms to ensure only user which submitted a file are able to retrieve the processed file.
- **Security Management:** The TOE implements flow control mechanisms to modify the flow and modification of files. This will be achieved with configuration files handled by the administrators.
- **Privacy:** The TOE will generate unique IDs for submitted files, which cannot be linked to the same user.
- **Protection of the TSF:** The TOE generates reliable timestamps for use in other security functions (particularly during the generation of audit logs).
- **Resource Utilisation:** The TOE ensures that file processing and enforcements of policies will be applied in a fail state and handle a user definable maximum processing quota.

The report concludes that the product has complied with the Evaluation Assurance Level (EAL) 2 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by AISEF and was completed on 10 October 2017.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled.

b) Configure and Operate the TOE according to the vendor's product administrator guidance.
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved.
d) Users of the TOE should ensure that sufficient hardening of the underlying operational environment has been performed prior to installation and use of the TOE.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Contents

Chapter 1 – Introduction

1.1 Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification results of the IT security evaluation of the Votiro Secure Data Sanitization Engine version 7.1 against the requirements of the Common Criteria (CC), Evaluation Assurance Level (EAL) 2

b) Provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref 1) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is Votiro Secure Data Sanitization Engine version 7.1

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Votiro Secure Data Sanitization Engine
Software Version	7.1
Platforms	Windows Server 2016
Prerequisite software	Microsoft Visual C++ 2013 redistributable package. Microsoft Visual C++ 2015 redistributable package. Microsoft .NET Framework 3.5.1 and 4.5.

Security Target	Security Target - Votiro Secure Data Sanitization Engine, Version 1.2, 07 September 2017 (Ref 1)
Evaluation Technical Report	Evaluation Technical Report Votiro Secure Data Sanitization Engine, dated 31 October 2017, Document reference EFS-T049-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Conformant and Part 3 Extended, April 2017, Version 3.1, Rev 5
Methodology	Common Methodology for Information Technology, April 2017 Security version 3.1, Rev 5
Conformance	EAL2
Sponsor	ICT and Digital government, Department of Finance Services & Innovation, NSW Government, Level 23 McKell Building, 2-24 Rawson Place, Sydney NSW 200
Developer	Votiro Cybersec 126 Yigal Aviv Street, Tel Aviv 67443, Israel
Evaluation Facility	BAE Systems Applied Intelligence 14 Childers Street Canberra ACT 2600

Chapter 2 – Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, security policies, and its secure usage.

2.2 Description of the TOE

The Target of Evaluation (TOE) is Votiro Secure Data Sanitization Engine version 7.1.
The TOE is a product that is designed to supplement the traditional sandboxing approach for securing files entering a network. It can help detect and prevent 0-day and other advanced threats that are designed to work around the general sandboxing approach. The sanitiser engines implement several proprietary methods of sanitising files such as disrupting malicious code by the introduction of noise or micro changes.

2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit:** The TOE generates and stores audit files for a variety of auditable events. These events record the identity of the user that caused the event to occur, the date and time, the success/failure of the event and any other pertinent information.
- **User Data Protection:** The TOE implements flow control mechanisms to ensure only user which submitted a file are able to retrieve the processed file.
- **Security Management:** The TOE implements flow control mechanisms to modify the flow and modification of files. This will be achieved with configuration files handled by the administrators.
- **Privacy:** The TOE will generate unique IDs for submitted files, which cannot be linked to the same user.
- **Protection of the TSF:** The TOE generates reliable timestamps for use in other security functions (particularly during the generation of audit logs).
- **Resource Utilisation:** The TOE ensures that file processing and enforcements of policies will be applied in a fail state and handle a user definable maximum processing quota.

2.4 TOE Architecture

The TOE consists of the following major architectural components: an API system, the SDS-WS (Secure Data Sanitization-Webservice) system and the Management System.

- The API system allows API calls to be made to the TOE for the submission of files for processing and enables periodic polling of the TOE via API calls for the status of the file. Once processing is complete another API call allows the submitter to retrieve the processed file.

- The SDS system of the TOE performs file inspection and processing in order to reduce the levels of active and malicious content within the submitted files. This can involve the removal of metadata, custom styles, printer settings and more.
- The management system of the TOE handles the initial configuration of the TOE and processes the XML files that are used to configure individual policy and file processing settings.

2.5 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per the Guidance - Votiro SDS User Guide, Version 7.1rA, June 2017 and Votiro SDS-WS CC Guidance Supplement v1.1, 11 September 2017 (Ref 5).

The scope of the evaluation was limited to those claims made in the Security Target (Ref 1).

2.5.1 Evaluated Functionality

All tests performed during the evaluation were taken from the CEM (Ref 4) and sufficiently demonstrate the security functionality of the TOE

2.5.2 Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref 6) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the New Zealand Information Security Manual (NZISM) (Ref 7).

The following components are considered outside of the scope of the TOE:

- The evaluator has found the initialisation of the TOE is handled by the underlying OS on which it is installed and therefore out of scope of this evaluation.

Email integration and virus inspection have not been tested as part of this evaluation.

2.6 Security

2.6.1 Security Policy

The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The Security Target (Ref 1) contains no explicit security policy statements.

2.7 Usage

2.7.1 Evaluated Configuration

The TOE consists of the Secure Data Sanitization Engine v7.1. The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the guidance documentation (Ref 5).

2.7.2 Secure Delivery

To ensure that the software received is the evaluated product the customer must check the version details received against the list specified in the TOE. The customer should perform the following checks to ensure that they have received the correct version of the TOE:

- Upon purchasing the SDS-WS from either Votiro Cybersec or an authorised reseller, the customer will be sent a username and twenty character randomly generated password in separate emails.
- This will allow the customer to login to the Votiro website and download the installer for the SDS webserver. Each download link provided includes an expected file name, file size and an MD5 hash in order to ensure that the download is genuine.

2.7.3 Installation of the TOE

The guidance documentation (Ref 5) contains all relevant information for the secure configuration of the TOE.

2.8 Version Verification

Version verification is completed as part of the installation procedure.

2.9 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The guidance documentation (Ref 5) contains all relevant information for configuring the TOE.
All common criteria guidance material is available at www.commoncriteriaportal.org.
The Information Security Manual (ISM) is available at www.asd.gov.au.

2.10 Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

Table 2 Assumptions Information

Assumption	Description
A.NO_EVIL	It is assumed that there will be one or more competent administrators assigned to manage the Votiro SDS server, its platform and the security of the information both of them contain. It is also assumed that the administrator(s) are not careless, wilfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation.
A.INSTALL	It is assumed that Votiro SDS is delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures.
A.PHYSICAL_PROTECT	It is assumed that Votiro SDS server and its associated platforms will be located within facilities providing controlled access to the TOE.
A.LOGICAL_PROTECT	The network environment in which the TOE is located ensures that only authorised users can are connect to it via its API. Thus the TOE is assumed to be deployed within a secure network environment.
A.TIME	The operational environment of the TOE will provide reliable time sources for use by the TOE.
A.CRYPTO	The operational environment of the TOE will provide approved cryptographic functions for use by the TOE.

Chapter 3 – Evaluation

3.1 Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3 (Refs 2 and 3).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 5 (Ref 4).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref 8) were also upheld.

The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from guidance (Ref 5).

3.3 Testing

3.3.1 Functional Testing

To gain confidence that the developers testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage, test plans and procedures and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.
All SFRs listed in the Security Target were exercised during testing.

3.3.2 Test phases

Testing was conducted between 13th to 15th of September 2017.

3.4 Penetration Testing

The Evaluators performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time)
b) Specialist technical expertise required (specialist expertise)
c) Knowledge of the TOE design and operation (knowledge of the TOE)
d) Window of opportunity
e) IT hardware/software or other equipment required for the exploitation.

Chapter 4 – Certification

4.1 Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the Certifiers.

4.2 Assurance

This certification is focused on the evaluation of product compliance with EAL 2. Agencies can have confidence that the scope of an evaluation against an EAL 2 covers the necessary security functionality expected of the evaluated product and known security threats will have been addressed.

EAL2 provide assurance by a full security target and an analysis of the SFR in that ST, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures. This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications. Compliance also provides assurance through evidence of secure delivery procedures.

4.3 Certification Result

After due consideration of the conduct of the evaluation as witnessed by the Certifiers and of the Evaluation Technical Report (Ref 9) the Australasian Certification Authority **certifies** the evaluation of the Votiro Secure Data Sanitization Engine version 7.1 product performed by the Australasian Information Security Evaluation Facility, BAE Applied Intelligence. BAE Applied Intelligence **has determined** that Votiro Secure Data Sanitization Engine version 7.1 uphold the claims made in the Security Target (Ref 1) and **has met** the requirements of the CC and CEM.
Certification is not a guarantee of freedom from security vulnerabilities.

4.4 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian

Government users should refer to ISM (Ref 6) and New Zealand Government users should consult the NZISM (Ref 7).

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled.
e) Configure and operate the TOE according to the vendor's product administrator guidance.
f) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved.
g) Users of the TOE should ensure that sufficient hardening of the underlying operational environment has been performed prior to installation and use of the TOE.

Annex A – References and Abbreviations

A.1 References

1. Security Target - Votiro Secure Data Sanitization Engine, Version 1.2, 07 September 2017

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

3. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5

4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1, Revision 5.

5. Guidance Documentation:

    5.1. Guidance - Votiro SDS User Guide, Version 7.1rA, June 2017

    5.2. Votiro SDS-WS CC Guidance Supplement v1.1, 11 September 2017

6. Australian Government Information Security Manual (ISM) https://www.asd.gov.au/infosec/ism/index.htm

7. NZ Information Security Manual (NZISM): https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/

8. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.

9. Evaluation Technical Report Votiro Secure Data Sanitization Engine, dated 31 October 2017, Document reference EFS-T049-ETR 1.0

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ACA	Australasian Certification Authority
API	Application Programming Interface
ASD	Australian Signals Directorate
CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
SDS	Secure Data Sanitisation
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy