PP-Configuration for Application Software, Endpoint Detection and Response, and Host Agent

Version: 1.0

2020-10-27

National Information Assurance Partnership

Contents

1 Introduction

1.1 Overview

This PP-Configuration is for a distributed software application that includes both Endpoint Detection and Response (EDR) and Host Agent capabilities. The EDR capability operates in either a cloud or an on-premises deployment via a physical or virtual operating system. The EDR capability interacts with one or more Host Agent applications installed on remote systems to collect endpoint host data to detect unauthorized activity and allow threat management. Each capability also enforces security functions that are applicable to generic software applications.

1.2 PP-Configuration Reference

This PP-Configuration is identified as follows:

- PP-Configuration for Application Software, Endpoint Detection and Response, and Host Agent, Version 1.0, 27 October 2020
- As a shorthand reference, it can be identified as “CFG_APP-EDR-HA_V1.0“

1.3 PP-Configuration Components Statement

This PP-Configuration includes the following components:

- Base-PP: Protection Profile for Application Software, Version 1.3 (PP_APP_V1.3)
- PP-Module: PP-Module for Endpoint Detection and Response, Version 1.0 (MOD_EDR_V1.0)
- PP-Module: PP-Module for Host Agent, Version 1.0 (MOD_HA_V1.0)

2 Conformance Claims

2.1 CC Conformance

Conformance Statement

To be conformant to this PP-Configuration, an ST must demonstrate Exact Conformance, as defined by the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

CC Conformance Claims

This PP-Configuration, and its components specified in Section 1.3, are conformant to Parts 2 (extended) and 3 (extended) of Common Criteria Version 3.1, Release 5 [CC].

2.2 SAR Statement

In order to evaluate a TOE that claims conformance to this PP-Configuration, the evaluator shall evaluate the TOE against the following SARs in Table 1 defined by the Base-PP.

Table 1: Base-PP SARs

Assurance Class	Assurance Components
Security Target (ASE)	Conformance Claims (ASE_CCL.1)
	Extended Components Definition (ASE_ECD.1)
	ST Introduction (ASE_INT.1)
	Security Objectives (ASE_OBJ.2)
	Derived Security Requirements (ASE_REQ.2)
	Security Problem Definition (ASE_SPD.1)
	TOE Summary Specification (ASE_TSS.1)
Development (ADV)	Basic Functional Specification (ADV_FSP.1)
Guidance Documents (AGD)	Operational User Guidance (AGD_OPE.1)
	Preparative Procedures (AGD_PRE.1)
Life Cycle Support (ALC)	Labeling of the TOE (ALC_CMC.1)
	TOE CM Coverage (ALC_CMS.1)
	Timely Security Updates (ALC_TSU_EXT.1)
Tests (ATE)	Independent Testing – Conformance (ATE_IND.1)
Vulnerability Assessment (AVA)	Vulnerability Survey (AVA_VAN.1)

The Supporting Documents included with the PP-Modules contain specific information with respect to the evaluation of the SARs listed in the table above. Similarly, the Base-PP contains “Evaluation Activities” in the PP itself that have the same type of information on how to evaluate the SARs.