CR-21-07

TACHYON Endpoint Security 5.5
인증보고서

인증번호 : ISIS-1077-2021

2021년 3월

IT보안인증사무국

1. 제품 개요

TACHYON Endpoint Security 5.5(이하 TOE)는 개인 사용자 PC에 존재하는 악성코드를 탐지하고 제거하여 PC에 저장된 중요 사용자 데이터를 보호하기 위한 안티바이러스 제품이다. TOE 및 TOE 구성요소는 다음과 같이 식별된다.

구분	식별자	형태 및 배포방법
TOE	TACHYON Endpoint Security 5.5	
소프트웨어	TACHYON Endpoint Security 5.5.1.2 · 설치파일 : TACHYONSetup_T5.5.exe 패턴버전 2020.02.12.02 · 설치파일 : TACHYONSetup_P5.5.exe	소프트웨어 형태로 온라인배포
지침서	TACHYON5.chm V2020.02.05.01	전자파일 형태로 도움말 링크를 통해 제공
설명서	TES_5.5_AGD_사용자설명서_v1.4.pdf	전자파일 형태로 담당자 E-mail로 배포

※ 안티바이러스 엔진: TACHYON 엔진 2020.02.12.02 Bitdefender 엔진 14241860

[표 1] TOE 구성요소 식별 정보

TOE는 다음의 제3자 제공제품을 포함한다.

- OpenSSL 1.1.1i : 업데이트 서버 - TOE, TACHYON Live 서버 – TOE, 신고 서버 – TOE 간 암호통신을 위한 라이브러리
- nProtect Crypto V1.1 : TSF데이터 암복호화를 위한 라이브러리
- BitDefender Core Anti-Malware SDK 14241860 : 자사의 TACHYON 엔진과 함께 악성코드 차단 클래스를 병행 지원하는 Bitdefender 사의 안티 바이러스 엔진
- SQLite V3.33.0 : 감사데이터 관리를 위한 File DBMS
- SQLCipher V4.4.2 : 감사데이터 암호화를 위한 라이브러리

TOE의 설치 및 운영에 필요한 하드웨어 및 소프트웨어 요구사항은 다음과 같다.

구분		사양
H/W	CPU	Intel(R) QuadCore 2.4 GHz 이상
	Memory	4 GB 이상
	HDD	TOE의 설치에 필요한 공간 5 GB 이상
	NIC	100/1000 Mbps Ethernet 1개
운영체제		Windows 7 Professional SP1 32/64bit Windows 10 Pro 32/64bit

[표 2] TOE의 설치 및 운영에 필요한 H/W 및 S/W 요구사항

인증 효력에 관한 고지: 상기 제품의 인증서는 IT보안인증사무국 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

2. 주요 기능

TOE가 제공하는 일반적인 보안 특성은 다음과 같다.

■ 악성코드 탐지

TOE는 수동/예약검사 및 실시간 검사 기반의 악성코드 탐지 기능을 제공하며, 이때 메모리 검사를 우선 수행한 이후 해당 검사 기능을 수행한다. TOE는 부트/파일기반 및 메모리 기반 바이러스 탐지 기능을 제공한다. 또한 TOE는 디스크에 저장되거나 메모리에 로드된 모든 파일(실행파일, 압축파일, 확장자가 변경된 실행파일, 실행 압축된 파일, 임시저장파일)에 포함된 웜, 트로이 목마 및 스파이웨어를 탐지하는 기능을 제공한다. TOE는 악성코드 탐지 시 에이전트가 설치된 PC 화면에 대응방법을 포함한 악성코드 탐지정보를 표시하며, 탐지 정보는 탐지일시, 악성코드 명, 대응 방법의 정보를 포함한다.

■ 악성코드 대응

TOE는 탐지된 바이러스에 대해, 부트 기반 바이러스에 대한 제거 기능과, 파일 기반 바이러스의 파일 격리 및 파일 삭제 기능, 메모리 기반 바이러스의 제거 및 프로세스 종료 기능을 제공한다. 또한 TOE는 탐지된 웜, 트로이목마, 스파이웨어를 삭제할 수 있는 기능을 제공한다.

■ 보안감사

TOE는 감사 기능의 시작/종료, 설정 변경내역, 보안기능 수행 내역에 대한 감사

데이터를 생성하며 사용자 PC에서의 악성코드 탐지/경고/대응, 자체보호 기능에 대한 감사기록도 포함한다. TOE는 감사기록 생성시 사건발생 일시, 사건유형, 사건을 발생시킨 주체의 신원, 작업 내역 및 결과(성공/실패) 정보를 포함한다. TOE는 저장된 감사기록에 대해 변경 및 삭제 기능을 제공하지 않는다. TOE는 감사증적의 크기가 지정된 한도를 초과할 경우 정의된 방식에 따라 사용자에게 통보하며, 감사증적 포화 시 오래된 감사 레코드 덮어쓰기를 수행하여 저장실패에 대응한다. TOE는 잠재적인 보안 위반을 탐지한 경우 대응행동을 수행한다.

■ 보안관리

TOE는 사용자에게 보안기능, 보안정책 및 중요 데이터 등을 설정 및 관리할 수 있는 보안관리 기능을 제공한다.

■ 전송 데이터 보호

TOE는 업데이트서버/Live서버/신고서버와 통신 시 암호화된 통신채널을 사용하여 전송데이터를 보호한다.

■ 자체시험

TOE는 제품의 정확한 운영을 보장하기 위하여 시동과 정규 운영 동안 주기적으로 실행한다. TOE는 사용자에게 TOE의 설정값 및 TOE 자체의 무결성을 검증하는 기능을 제공한다.

■ 에이전트 보호

TOE는 정상적인 동작을 보장하기 위한 자체 보호 기능을 제공한다.

■ 에이전트와 서버 간 안전한 연동

TOE는 업데이트 서버 주소에 대한 무결성 검증을 수행하며, 업데이트 서버로부터 받은 파일에 대해 전자서명 검증을 수행한다.

※ 상기 제품은 인증서에 명시된 국가용 보안요구사항 제품 유형으로 인증되었으며, 국가용 보안요구사항을 준수하여 구현된 보안기능에 대한 세부 설명 및 국가용 보안요구사항에 포함되지 않은 부가기능은 설명서를 참조한다. 관련 부가기능은 설명서에 기반하여 기능시험 되었으며, 제품 취약성 분석 시 포함되었다. 다만, 부가기능은 인증된 제품 유형과 무관하다.

3. 평가결과 요약

TOE에 대한 평가는 한국기계전기전자시험연구원에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부의 EAL3 평가보증등급을 만족하여, 공통평가기준 1부 245항에 따라 “적합”한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가인증지침 (2017. 8. 24) 정보보호제품 평가인증 수행규정 (2017. 9. 12)
평가제품	TACHYON Endpoint Security 5.5
보호프로파일	없음
보안요구사항	안티바이러스 제품 보안요구사항 V1.0
보안목표명세서	TACHYON Endpoint Security 5.5 보안목표명세서 V1.4 (2021.03.02)
평가보고서	TACHYON Endpoint Security 5.5 평가결과보고서 V2.0 (2021.03.02)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R2
평가방법론	정보보호시스템 공통평가방법론 V3.1 R2
검증필 암호모듈	없음
평가신청인	㈜잉카인터넷
개발업체	㈜잉카인터넷
평가기관	한국기계전기전자시험연구원