CR-20-34

TACHYON Total Security 3.5
인증보고서

인증번호 : ISIS-1020-2020

2020년 6월

IT보안인증사무국

1. 제품 개요

TACHYON Total Security 3.5(이하 TOE)는 개인 사용자 PC(PC기반 서버 포함)에 존재하는 악성코드를 탐지하고 제거하여 PC에 저장된 중요 사용자 데이터를 보호하기 위한 안티바이러스 제품이다.

TOE 및 TOE 구성요소는 다음과 같이 식별된다.

구분	식별자	배포형태
TOE	TACHYON Total Security 3.5	
TOE 세부버전	3.5.0.0200	
TOE 구성요소	TTSS (세부 버전: 3.5.0.0100) · TACHYONSetup_TTSS3.5.0.0100.exe · TACHYONSetup_TTSS3.5.0.0100.tar	소프트웨어 형태로 온라인 배포
	TTSA (세부 버전: 3.5.0.0100) · TACHYONSetup_TTSA3.5.0.0100.exe	
	TACHYON Endpoint Security 5.5 (세부 버전: 5.5.0.1) · TACHYONSetup_TES5.5.0.1.exe	
	TACHYON Server Security 5.5 (세부 버전: 5.5.0.1) · TACHYONSetup_TSS5.5.0.1.exe	
설명서	TACHYON5.chm V2020.02.05.01	전자파일 형태로 TTSS의 관리자 페이지에서 제공
	TTS3.5_AGD_서버설치설명서_v1.5.pdf TTS3.5_AGD_관리자서버설명서_v1.1.pdf TTS3.5_AGD_관리자에이전트설명서_v1.1.pdf TES5.5_AGD_TES(TSS) 사용자설명서_v1.2.pdf	전자파일 형태로서, 담당자 E-mail로 배포

※ 안티바이러스 엔진: TACHYON 엔진 2020.02.12.02 Bitdefender 엔진 14241860

[표 1] TOE 구성요소 식별 정보

TOE는 보안기능성을 제공하기 위해 다음과 같은 제3자 제공 제품을 포함한다.

TOE 구성요소	구분	용도
TTSS	nProtect Crypto V1.1	TSF데이터 암복호화를 위한 라이브러리
	Spring security 4.2.3	TSF데이터 해시화를 위한 라이브러리
	OpenSSL 1.1.1d	TTSS - TTSA 간 암호통신을 위한 라이브러리 TTSS - 업데이트 서버(모듈, 엔진) 간 암호통신을 위한 라이브러리
TTSA	OpenSSL 1.1.1d	TTSS - TTSA 간 암호통신을 위한 라이브러리
	nProtect Crypto V1.1	감사데이터, TSF데이터 암복호화를 위한 라이브러리

TOE 구성요소	구분	용도
TES / TSS	OpenSSL 1.1.1d	TACHYON Live 서버 - TES/TSS, 신고서버 - TES/TSS 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 V3.30.1	감사데이터 관리를 위한 File DBMS
	SQLCipher V4.3.0	감사데이터 암호화를 위한 라이브러리

[표 2] TOE에 포함된 제3자 제공 제품

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

구성요소	구분		사양
TTSS	H/W	CPU	Intel(R) QuadCore 3.0 GHz 이상
		Memory	8 GB 이상
		HDD	TTSS의 설치에 필요한 공간 5 GB 이상
		NIC	1000 Mbps Ethernet 1개
	운영체제		CentOS 6.9 kernel 2.6.32 64bit CentOS 7.5 kernel 3.10.0 64bit Windows Server 2008 R2 Standard SP1 64bit Windows Server 2012 R2 Standard 64bit Windows Server 2016 Standard 64bit
	소프트웨어		JDK 8u242 / JRE 8u242 MariaDB 10.3.8 Tomcat 8.5.53 Apache 2.4.41 Redis 3.2.100 Mod_jk 1.2.46 Mod_Log_rotate 1.0.2 Visual Studio Visual C++ 2015 x64 14.0.23026
TTSA	H/W	CPU	Intel(R) QuadCore 2.4 GHz 이상
		Memory	4 GB 이상
		HDD	TTSA의 설치에 필요한 공간 2 GB 이상
		NIC	100/1000 Mbps Ethernet 1개
	운영체제		Windows 7 Professional SP1 32/64bit Windows 8.1 Pro 32/64bit Windows 10 Pro 32/64bit Windows Server 2008 R2 Standard SP1 64bit Windows Server 2012 Standard 64bit Windows Server 2012 R2 Standard 64bit Windows Server 2016 Standard 64bit

구성요소	구분		사양
TACHYON Endpoint Security 5.5	H/W	CPU	Intel(R) QuadCore 2.4 GHz 이상
		Memory	4 GB 이상
		HDD	TES의 설치에 필요한 공간 5 GB 이상
		NIC	100/1000 Mbps Ethernet 1개
	운영체제		Windows 7 Professional SP1 32/64bit Windows 8.1 Pro 32/64bit Windows 10 Pro 32/64bit
TACHYON Server Security 5.5	H/W	CPU	Intel(R) QuadCore 2.4 GHz 이상
		Memory	4 GB 이상
		HDD	TSS의 설치에 필요한 공간 5 GB 이상
		NIC	100/1000 Mbps Ethernet 1개
	운영체제		Windows Server 2008 R2 Standard SP1 64bit Windows Server 2012 Standard 64bit Windows Server 2012 R2 Standard 64bit Windows Server 2016 Standard 64bit

※ TTSA와 TACHYON Endpoint Security 5.5은 동일한 PC에 설치되어 운영되어야 함

※ TTSA와 TACHYON Server Security 5.5은 동일한 서버에 설치되어 운영되어야 함

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

인가된 관리자가 TOE에 접속하여 보안관리를 수행하기 위해 요구되는 PC의 최소사항은 다음과 같다.

구분	사양
소프트웨어	Internet Explorer 11.0.31 이상 또는 Chrome 68.0.3440.106 이상

[표 3] 관리자 PC의 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

TES/TSS는 수동/예약검사 및 실시간 검사 기반의 악성코드 탐지 기능을 제공하며, 이때 메모리 검사를 우선 수행한 이후 해당 검사 기능을 수행한다. TES/TSS는 부트/파일기반 및 메모리 기반 바이러스 탐지 기능을 제공한다. 또한 TES/TSS는 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. TES/TSS는 악성코드 탐지 시 관리자의 보안 화면 및 에이전트가 설치된 PC 화면에 대응방법을 포함한 악성코드 탐지정보를 표시하며, 탐지 정보는 탐지일시, 악성코드 명, 대응 방법의 정보를 포함한다.

■ 악성코드 대응

TES/TSS는 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 TES/TSS는 탐지된 웜, 트로이목마, 스파이웨어를 삭제할 수 있는 기능을 제공한다.

■ 보안감사

TTSS는 인가된 관리자에게 웹 인터페이스를 통한 감사데이터 조회 기능을 제공하며, 감사데이터는 사건발생 일시, 사건유형, 사건을 발생시킨 주체의 신원, 작업 내역 및 결과(성공/실패) 정보를 포함한다. TTSS는 감사증적의 크기가 지정된 한도를 초과할 경우 관리자에게 이메일 및 경고창을 통하여 경고메세지를 발송하며, 감사증적 포화 시 오래된 감사 레코드 덮어쓰기를 수행하여 저장실패에 대응한다. TTSS는 잠재적인 보안 위반이 탐지되는 경우 인가된 관리자에게 경고창 및 이메일을 통하여 경보메시지를 발송한다.

■ 식별 및 인증

TTSS는 관리자에게 식별 및 인증기능을 제공한다. TTSS는 관리자의 인증실패 횟수가 지정된 값에 도달 시, 설정된 시간동안 식별 및 인증 기능을 비활성 한다. TTSS는 식별 및 인증을 시도하는 관리자의 비밀번호를 마스킹하여 보호한다. TTSS는 관리자의 인증세션 정보에 대한 재사용을 방지한다.

■ 보안관리

TTSS는 인가된 관리자에게 보안기능, 보안정책 설정 및 관리할 수 있는 보안관

리 기능을 웹 인터페이스를 통해 제공한다. TOE의 관리자 페이지는 사전 등록된 IP 주소에서만 접속 가능하다. TOE는 각 사용자 PC에 설치된 안티바이러스 에이전트와 관리 서버간 정상 통신 여부를 확인할 수 있는 기능을 제공한다.

■ 전송 데이터 보호

TOE는 TOE 관리페이지 접속, 업데이트(모듈, 엔진) 서버와 TTSS 간 통신 시, 관리서버(TTSS)와 에이전트(TTSA)간 통신 시, 라이브 서버와 에이전트(TES/TSS)간 통신 시, 신고 서버와 에이전트(TES/TSS)간 통신 시 암호화 통신 채널을 사용하여 전송데이터를 보호한다.

■ 자체시험

TOE는 제품의 정확한 운영을 보장하기 위하여 시동 시, 정규 운영 동안 주기적으로, 업데이트 파일 다운로드 및 업데이트 완료 시 주기적으로 TSF 데이터 및 TSF 실행파일에 대하여 자체시험을 실행한다. TOE는 인가된 관리자 및 사용자에게 수동으로 TOE의 설정값 및 TOE 자체의 무결성을 검증하는 기능을 제공한다.

■ 안전한 세션관리

TTSS는 관리자 로그인 이후 비활동 시간이 지정된 한도에 도달할 경우, 해당 관리자 세션을 종료한다. TTSS는 관리자 로그인 이후 다른 단말에서 동일 계정으로 중복 로그인 시 이전 접속을 종료한다.

■ 에이전트 보호

TTSA/TES/TSS는 정상적인 동작을 보장하기 위한 자체 보호 기능을 제공한다.

■ 안티바이러스 에이전트와 서버 간 안전한 연동

TTSA/TES/TSS는 관리서버의 주소에 대한 무결성 검증을 수행하며, 관리서버로부터 받은 파일의 전자서명 검증은 TTSA/TES/TSS가 각각 구성요소에 해당하는 파일에 대해 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 Total Security 3.5
보호프로파일	없음
보안요구사항	안티바이러스 제품 보안요구사항 V1.0
보안목표명세서	TACHYON Total Security 3.5 보안목표명세서 V1.5 (2020.06.17)
평가보고서	TACHYON Total Security 3.5 평가결과보고서 V3.0 (2020.06.17)
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