CR-23-07

Secuve TOS 5.0 for Unix (Solaris 11)

인증보고서

인증번호 : CISS-1213-2023

2023년 2월

IT보안인증사무국

1. 제품 개요

Secuve TOS 5.0 for Unix (Solaris 11)(이하 TOE)는 보호하고자 하는 서버의 중요 자원(파일, 디렉터리, 프로세스 등)에 대한 접근을 정해진 규칙에 따라 허용하거나 거부하여 조직 내부의 주요 자원을 불법적 침해로부터 보호하는 목적으로 사용되는 서버 접근통제 제품이다. TOE 및 TOE 구성요소는 다음과 같이 식별된다.

<table>
<tr><th colspan="3">구분</th><th colspan="2">식별정보</th><th>유형</th><th>배포 형태</th></tr>
<tr><td colspan="3">TOE</td><td colspan="2">Secuve TOS 5.0 for Unix (Solaris 11)</td><td rowspan="8">SW</td><td rowspan="13">CD/ 인편 전달</td></tr>
<tr><td colspan="3">릴리즈 버전</td><td colspan="2">rev0001</td></tr>
<tr><td rowspan="6">TOE 구성요소</td><td>에이전트 시스템</td><td colspan="2">Secuve TOS 5.0 Agent 5.0.17 Solaris 11 (Build Date 20221104)
- Secuve_TOS_5.0_Agent_for_Solaris11_5.0.17_20221104.tar.Z</td></tr>
<tr><td rowspan="5">매니저 시스템</td><td>관리콘솔 (TOSMS)</td><td>Secuve TOS 5.0 TOSMS 5.0.17 (Build Date 20221123)
- Secuve_TOS_5.0_TOSMS_5.0.17_20221123.tar</td></tr>
<tr><td>ScvCA</td><td>Secuve TOS 5.0 ScvCA 5.0.17 (Build Date 20221104)
- Secuve_TOS_5.0_ScvCA_5.0.17_20221104.tar.Z</td></tr>
<tr><td>ScvEA</td><td>Secuve TOS 5.0 ScvEA 5.0.17 (Build Date 20221110)
- Secuve_TOS_5.0_ScvEA_5.0.17_20221110.tar</td></tr>
<tr><td>LogServer</td><td>Secuve TOS 5.0 LogServer 5.0.17 (Build Date 20221110)
- Secuve_TOS_5.0_LogServer_5.0.17_20221110.tar</td></tr>
<tr><td>Secuve Auth Client</td><td colspan="2">Secuve Auth Client 1.0.2 (Build Date 20221123)
- Secuve_Auth_Client_1.0.2_20221123.zip</td></tr>
<tr><td colspan="3" rowspan="3">설명서</td><td colspan="2">Secuve TOS 5.0 for Unix (Solaris 11) 준비절차서 V1.1
- 준비절차서(1.1)-평가인증실-20221221.pdf</td><td rowspan="3">전자 파일 (PDF)</td></tr>
<tr><td colspan="2">Secuve TOS 5.0 for Unix (Solaris 11) 관리자설명서 V1.1
- 관리자설명서(1.1)-평가인증실-20221221.pdf</td></tr>
<tr><td colspan="2">Secuve TOS 5.0 for Unix (Solaris 11) 사용자설명서 V1.0
- 사용자설명서(1.0)-평가인증실-20220913.pdf</td></tr>
</table>

TOE는 보안기능성을 제공하기 위해 다음과 같은 3rd Party 요소를 포함한다.

- OpenSSL 1.1.1s : TOE 구성요소 간 전송되는 데이터 보호 및 저장데이터 보호에 사용
- Clipreport 4.0 : 로그 리포트 조회에 사용

- Highcharts 9.2.2: 웹 브라우저를 통하여 관리콘솔 홈 화면에 관리대상시스템 운영 및 자원모니터링 현황 데이터를 시각화 표현에 사용

TOE를 운영하기 위해 요구되는 하드웨어 및 소프트웨어 요구사항은 다음과 같다.

- 매니저시스템

구분		최소사양
하드웨어	CPU	Intel Xeon® CPU E5620 @ 2.40GHz 이상
	RAM	32GB 이상
	HDD	TOE(매니저시스템) 설치에 필요한 공간 198MB 이상
	NIC	TCP / IP 기반 네트워크 10/100/1000 Base-T Ethernet Card 1개 이상
운영체제		Red Hat Enterprise Linux release 8.7 (Ootpa) 4.18.0-425.3.1.el8.x86_64 (커널버전)
필수 소프트웨어		Apache-tomcat-9.0.70
		Java Runtime Environment 1.8.0_351
		DBMS (Tibero 6.0)

- 에이전트시스템

구분		최소사양
하드웨어	CPU	SPARC-S7 (4267 MHz, 8core) 이상
	RAM	4GB 이상
	HDD	TOE(에이전트시스템) 설치에 필요한 공간 66MB 이상
	NIC	TCP / IP 기반 네트워크 10/100/1000 Base-T Ethernet Card 1개 이상
운영체제		Oracle Solaris 11 (64bit)

- Secuve Auth Client

구분		최소사양
하드웨어	CPU	Intel(R) Core(TM) i5-5200U CPU @ 2.20GHz 이상
	RAM	8GB 이상
	HDD	TOE(Secuve Auth Client) 설치에 필요한 공간 15.9MB 이상
	NIC	TCP / IP 기반 네트워크

구분		최소사양
		10/100/1000 Base-T Ethernet Card 1개 이상
운영체제		Windows 10 Pro (32bits/64bits) Windows 11 Pro (64bits)
필수 소프트웨어		Visual Studio C++ 2008 재배포 가능 패키지 (vcredist_x86_2008.exe)

- 관리자 PC

구분	최소사양
필수 소프트웨어	Microsoft Edge 108.0 또는 Chrome 108.0

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

2. 주요기능

TOE가 제공하는 주요 보안기능은 다음과 같다.

■ 자원 접근통제

TOE(에이전트시스템)는 인가된 관리자가 설정한 강제적 접근통제 정책 및 임의적 접근통제 정책에 근거하여 등급기반 방식의 접근통제를 수행한다. 또한, TOE(에이전트시스템)는 인가된 관리자가 설정한 역할기반 접근통제 정책에 근거하여 역할기반 방식의 접근통제를 수행한다. TOE(에이전트시스템)는 역할기반 방식의 접근통제를 수행하기 위해 역할관리, 역할검토 기능을 제공한다. TOE(에이전트시스템)는 사용자, 그룹, 역할 등에 대해 기존에 할당된 권한 또는 접근허가를 회수하는 경우 자원에 대한 모든 이전 정보 내용이 가용하지 않도록 한다.

■ 감사 기록

TOE는 정의된 감사대상 사건 발생 시, 사건 발생 일시, 보안기능 수행내역 등을 포함하여 감사데이터를 생성하며, 인가된 관리자에게 감사데이터를 논리적 관계 기준에 따라 검토하는 기능을 제공한다. TOE(매니저시스템, 에이전트시스템)는 잠재적인 보안 위반을 탐지한 경우 인가된 관리자가 설정한 대응행동을 수행한다. TOE(매니저시스템, 에이전트시스템)는 저장된 감사 레코드를 비인가된 삭제 및 변경으로부터 보호하며, 감사증적의 크기가 지정된 한도를 초과하는 경우 사전 정의한 방식으로 인가된 관리자에게 통보하고, 감사증적이 포화될 경우 저장 실패에 대응하는 기능을 제공한다.

■ 식별 및 인증

TOE(매니저시스템)는 인가된 관리자의 신원을 검증하기 위하여 ID/패스워드 등을 사용하여 식별 및 인증을 수행하고, 식별 및 인증 실패 시 인증 실패 대응 기능을 제공한다. TOE(매니저시스템)는 패스워드 등록 시 조합 규칙을 만족하는지 검증하며, 인증 진행 시 패스워드를 마스킹하여 보호한다.

■ 보안관리

TOE(매니저시스템)는 인가된 관리자가 보안기능, 보안정책 등을 설정하고 관리할 수

있는 보안관리 기능을 제공한다.

■ 전송 데이터 보호

TOE는 물리적으로 분리된 매니저시스템, 에이전트시스템, Secuve Auth Client간에 전송되는 데이터를 암호화를 통해 보호한다. 또한, 인가된 관리자가 TOE(매니저시스템)에 접속 시 안전한 암호통신 프로토콜을 사용한다.

■ 자체 시험

TOE는 정확한 운영을 보장하기 위해 시동시 및 정규 운영 동안 주기적으로 자체시험을 실행하고, 인가된 관리자에게 TOE 설정값 및 TOE 자체의 무결성을 검증하는 기능을 제공한다.

■ 안전한 세션 관리

TOE(매니저시스템)는 인가된 관리자 로그인 이후 일정 시간 동안 동작하지 않는 경우 세션 종료 기능을 수행하며, 인가된 관리자 로그인 이후 동일 계정 또는 동일 권한으로 다시 로그인을 시도하는 경우 이전 접속을 종료한다.

※ 상기 제품은 인증서에 명시된 국가용 보안요구사항 제품 유형으로 인증되었으며, 국가용 보안요구사항을 준수하여 구현된 보안기능에 대한 세부 설명, 제품의 운영환경 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 한국정보통신기술협회에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부의 EAL4 평가보증등급을 만족하여, 공통평가기준 1부 245항에 따라 “적합”한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가·인증 등에 관한 고시 (2022. 10. 31.) 정보보호제품 평가·인증 수행규정 (2021. 5. 17.)
평가제품	Secuve TOS 5.0 for Unix (Solaris 11)
보호프로파일	없음
보안요구사항	서버 접근통제 제품 보안요구사항 V1.0
보안목표명세서	Secuve TOS 5.0 for Unix (Solaris 11) 보안목표명세서 V1.2
평가보고서	Secuve TOS 5.0 for Unix (Solaris 11) 평가결과보고서 V1.1
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R2
평가방법론	정보보호시스템 공통평가방법론 V3.1 R2
검증필 암호모듈 (탑재 필수)	해당 없음
평가신청인	㈜시큐브
개발업체	㈜시큐브
평가기관	한국정보통신기술협회