KECS-CR-23-70

CubeOne V3.0
인증보고서

인증번호 : KECS-CISS-1276-2023

2023년 11월

IT보안인증사무국

1. 제품 개요

CubeOne V3.0(이하 TOE)은 보호대상 데이터베이스를 암호화하여 보호하고자 하는 정보의 비인가된 노출을 방지하는 기능을 제공하는 데이터베이스 암호화 제품으로 소프트웨어 형태로 제공된다.

구분	식별자		배포형태
TOE	CubeOne V3.0		
버전	rev.0025		
TOE 구성요소	CubeOne Manager	CubeOne_Manager_V3.0.00.03 · CubeOne_Manager_V3.0.00.03.exe	CD 배포에 포함
	CubeOne Server	[Plug-In 방식] CubeOne_Server_V3.0.00.03_L64_4.18_OR19C · CubeOne_Server_V3.0.00.03_L64_4.18_OR19C.tar CubeOne_Server_V3.0.00.03_A64_7.2_DB11.5 · CubeOne_Server_V3.0.00.03_ A64_7.2_DB11.5.tar CubeOne_Server_V3.0.00.03_L64_4.18_TI7 · CubeOne_Server_V3.0.00.03_L64_4.18_TI7.tar CubeOne_Server_V3.0.00.03_L64_4.18_MY8 · CubeOne_Server_V3.0.00.03_L64_4.18_MY8.tar CubeOne_Server_V3.0.00.03_W64_10_MS19 · CubeOne_Server_V3.0.00.03_W64_10_MS19.exe [API 방식] CubeOne_Server_V3.0.00.03_A64_7.2_API · CubeOne_Server_V3.0.00.03_A64_7.2_API.tar CubeOne_Server_V3.0.00.03_S64_5.11_API · CubeOne_Server_V3.0.00.03_S64_5.11_API.tar CubeOne_Server_V3.0.00.03_H64_B.11.31_API · CubeOne_Server_V3.0.00.03_H64_B.11.31_API.tar CubeOne_Server_V3.0.00.03_L64_4.18_API · CubeOne_Server_V3.0.00.03_L64_4.18_API.tar CubeOne_Server_V3.0.00.03_W64_10_API · CubeOne_Server_V3.0.00.03_W64_10_API.exe	CD 배포에 포함
	CubeOne Security Server	CubeOne_SServer_V3.0.00.03_L64_4.18_MY · CubeOne_SServer_V3.0.00.03_L64_4.18_MY.tar	CD 배포에 포함
설명서	CubeOne_OPE_V3.0.0.3 · CubeOne_OPE_V3.0.0.3.pdf		인쇄물, CD 배포에 포함
	CubeOne_PRE_V3.0.0.4 · CubeOne_PRE_V3.0.0.4.pdf		

[표 1] TOE 구성요소 식별 정보

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

구분	하드웨어 최소사양				
CubeOne Manager	CPU	Intel Core 2 Duo 2.40 GHz 이상			
	Memory	4 GB 이상			
	HDD	TOE 설치에 필요한 공간 200 MB 이상			
	NIC	10/100/1000 Mbps X 1 Port 이상			
	OS	Windows Server 2019 (64 bit)			
CubeOne Server (Plug-In 방식)	CPU	POWER7 3.0 GHz 이상	Intel Dual Core 1.8 GHz 이상	Intel Dual Core 1.8 GHz 이상	
	Memory	4 GB 이상			
	HDD	TOE 설치에 필요한 공간 200 MB 이상			
	NIC	10/100/1000 Mbps X 1 Port 이상			
	OS	AIX 7.2 (64 bit)	Rocky Linux 8.7 (64 bit) (kernel 4.18.0)	Windows Server 2019 (64 bit)	
	DBMS	DB2 11.5	Oracle 19c, Tibero 7, Mysql 8.0.35	MSSQL 2019	
CubeOne Server (API 방식)	CPU	POWER7 3.0 GHz 이상	sparcv9 2848 MHz 이상	Intel(R) Itanium 2 1.6 GHz 이상	Intel Dual Core 1.8 GHz 이상	Intel Dual Core 1.8 GHz 이상
	Memory	4 GB 이상				
	HDD	TOE 설치에 필요한 공간 200 MB 이상				
	NIC	10/100/1000 Mbps X 1 Port 이상				
	OS	AIX 7.2 (64 bit)	SunOS 5.11 (64 bit)	HP-UX B.11.31 (64 bit)	Rocky Linux 8.7 (64 bit) (kernel 4.18.0)	Windows Server 2019 (64 bit)
CubeOne Security Server	CPU	Intel Core 2 Duo 2.26 GHz 이상				
	Memory	4 GB 이상				
	HDD	TOE 설치에 필요한 공간 200 MB 이상				
	NIC	10/100/1000 Mbps X 1 Port 이상				
	OS	Rocky Linux 8.7 (64 bit) (kernel 4.18.0)				
	필수 S/W	Mysql 8.0.35 Apache tomcat 9.0.82				

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

인가된 로그 관리자가 CubeOne Security Server에 접속하여 보안 관리 기능을 수행하기 위한 시스템의 최소 요구사항은 아래의 [표 2]와 같다.

구분	사양
S/W	Chrome V118.0 (64-bit)

[표 3] 관리자 PC 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.

■ 보안감사

TOE는 암호지원, 식별 및 인증 등 감사대상 사건에 따라 감사 레코드를 생성하고, 감사 레코드는 사건 일시, 사건 유형, 신원, 사건 결과를 포함한다. TOE의 시동 및 종료와 보안관련 설정 행위 등에 대하여 감사기록을 생성하며, 생성된 감사 기록을 인가되지 않은 삭제로부터 보호한다. 인가된 관리자만이 감사데이터를 조회할 수 있으며, 감사데이터 조회 시 선택적으로 조회가 가능하다. 감사된 사건 중 관리자 인증 실패 사건 발생, 무결성 위반 등 잠재적인 위반을 분석하여 인가된 관리자에게 경고화면 및 팝업으로 알람을 제공한다. 또한, 감사저장소가 초과할 경우 관리자에게 경고화면으로 알람을 제공하며, 감사 증적이 포화된 경우 CubeOne Manager는 감사된 사건을 무시하고, CubeOne Security Server은 가장 오래된 감사데이터를 덮어쓴다.

■ 암호지원

TOE는 암호키 관리 및 암호연산, 난수발생을 지원한다. 암호키 생성에는 검증필 암호모듈(COLib V1.2.0)의 난수발생기를 통해 난수를 사용하여 암호키를 생성하고, 보호대상 DBMS내의 사용자 데이터를 암호화하는데 검증필 암호모듈의 암호알고리즘을 사용한다. 또한, 저장된 TSF 데이터 보호를 위해 해시 알고리즘 및 대칭키 암호화를 사용하며, 전송 TSF 데이터 보호를 위해 해시알고리즘 및 대칭키 암호화를 사용하여 연산한다. 암호키 파기 시에는 메모리 영역을 '0'으로 3회 덮어씌워 파기를 수행한다.

■ 사용자 데이터 보호

사용자 데이터 암·복호화시 컬럼 별 암·복호화 기능을 제공하며, 암호화 후 평문인 원본 사용자 데이터를 '0'으로 3회 덮어쓰워 완전한 삭제를 수행하여 이전 정보 내용이 가용하지 않음을 보장한다.

■ 식별 및 인증

CubeOne Manger의 정책 관리자 및 CubeOne Security Server의 로그 관리자는 ID 및 PW 기반으로 신원을 식별 및 인증을 수행하며, 연속된 인증 실패 5회 도달 시 5분 동안 해당 관리자 계정 잠금 기능을 제공한다. 인증을 수행하는 동안 발생하는 피드백을 보호하고 인증실패에 대한 사유를 제공하지 않으며, 관리자 인증 및 패스워드 생성/변경 시 비밀정보가 정의된 보안성 기준(길이 및 조합규칙)을 만족시키는지 여부에 대한 검증을 수행한다. CubeOne Manager와 CubeOne Security Server는 인증데이터의 재사용을 방지한다. TOE의 구성요소 CubeOne Manger, CubeOne Server, CubeOne Security Server 간 통신 전 자체 인증 프로토콜을 통해 상호인증을 수행한다.

■ 보안 관리

TOE에서 사용자는 보안정책을 설정할 수 있는 정책 관리자와 보안경보 및 감사데이터 등을 조회할 수 있는 로그 관리자로 구분된다. 정책 관리자는 CubeOne Manager의 접속하여 보안관리를 수행하며, 로그 관리자는 CubeOne Security Server에 접속하여 보안관리를 수행한다. CubeOne Manager 인증시 사용되는 ID 및 패스워드는 설치과정에서 등록할 수 있고, CubeOne Security Server 인증시 사용되는 패스워드는 설치과정에서 등록할 수 있다.

■ TSF 보호

TOE는 TSF에 의해 통제되는 저장소에 저장되는 TSF 데이터의 노출 및 변경으로부터 보호하기 위해 검증필 암호모듈의 대칭키 암호알고리즘 및 메시지인증 알고리즘을 통해 암호화하여 저장한다. TOE 구성요소 간 (CubeOne Manger, CubeOne Server, CubeOne Security Server) 전송되는 TSF 데이터를 보호하기 위해 검증필 암호모듈의 대칭키 암호알고리즘 및 해시함수를 통해 암호화 통신을 수행한다. TSF 자체시험을 통하여 TOE의 주요 프로세스에 정상 구동 여부를 점검한다. TOE는 주요 프로세스에 대해 TOE 시동 시, 정규 운영 동안 주기적으로 자체시험을 수행하며, TOE 설정파일 및 주요 프로세스에 대한 무결성 검사를 TOE 시동 시, 정책 관리자 요청 시 수행한 후 무결성이 손상된 경우 관리자에게 경고 알람을 제공한다.

■ TOE 접근

CubeOne Manger의 정책 관리자 및 CubeOne Security Server이 로그 관리자는 접속 가능 IP로 지정된 단말에서만 관리접속 세션을 허용한다. 인가된

CubeOne Manger의 정책 관리자가 로그인 후 일정시간 활동이 없는 경우 세션이 잠기고 관리자 재인증을 해야 보안기능을 수행할 수 있으며, 인가된 CubeOne Security Server의 로그 관리자가 로그인 후, 일정시간 활동이 없는 경우 세션이 종료된다. 관리자의 관리접속에 대한 동시 세션은 최대 1명으로 제한한다.

3. 평가결과 요약

TOE에 대한 평가는 한국시스템보증에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부를 만족하고 국가용 보호프로파일을 준수하여, 공통평가기준 1부 330항에 따라 “적합”한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가인증 등에 관한 고시 (2022. 10. 31.) 정보보호제품 평가인증 수행규정 (2021. 5. 17)
평가제품	CubeOne V3.0
보호프로파일	국가용 데이터베이스 암호화 보호프로파일 V1.1 (2019.12.11)
보안요구사항	없음
보안목표명세서	CubeOne V3.0 보안목표명세서 V3.0.0.5 (2023.11.22)
평가보고서	CubeOne V3.0 평가결과보고서 V2.00 (2023.11.24)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R5
평가방법론	정보보호시스템 공통평가방법론 V3.1 R5
검증필 암호모듈 (탑재 필수)	COLib V1.2.0 (CM-231-2028.6)
평가신청인	㈜이글로벌시스템
개발업체	㈜이글로벌시스템
평가기관	한국시스템보증㈜