[붙임2] 취약점 분석 · 평가 기준 점검항목

□ 관리적 분야

분류	번호	취약점 점검 항목	등급
정보보호 정책	A-1	조직 전반에 적용하고 있는 정보보호 정책/지침 수립 및 경영진의 승인 획득	상
	A-2	정보보호 정책의 시행을 위해 필요한 방법, 절차, 주기 등을 정의하고 문서화	상
	A-3	정보보호 정책 및 시행문서를 모든 임직원 및 관련자에게 접근하기 쉬운 형태로 제공	상
	A-4	정보보호 정책 및 시행문서에 대한 타당성을 주기적으로 또는 중대한 변화 발생 시 검토·평가하여 수정 및 보완	상
	A-5	정보보호 정책 및 시행문서의 제·개정 시 이해관계자의 검토를 받고 해당 내용 반영	상
	A-6	연도별 정보보호 업무 세부추진 계획을 수립·이행	상
	A-7	기관의 정보보호 강화를 위한 중장기(3년 이상) 계획 수립·이행	상
정보보호 조직	A-8	정보보호 활동을 계획, 실행, 검토하는 전담 조직 및 담당자 구성	상
	A-9	정보보호위원회가 구성되어 있으며 위원회의 역할 및 책임을 문서화	상
자산 관리	A-10	주요정보통신기반시설 내 자산(인력, 시설, 장비 등)을 식별하여 자산분류기준을 수립하고 문서화	상
	A-11	정보자산을 보안등급과 중요도 등에 따라 분류하여 관리	상
	A-12	조직의 주요 자산 목록을 작성하고, 정기적인 자산 현황 조사 결과 및 변경 사항(취득, 폐기, 양도 등) 등을 자산 목록에 반영하여 변경이력을 최신으로 유지 관리	상
	A-13	자산의 등급에 따른 취급절차(생성·도입, 저장, 이용, 파기) 및 보호대책을 수립·이행	상
	A-14	정보자산별로 관리자 및 관리 책임자가 지정되어 있으며, 목록을 최신으로 유지·관리	상
위험 관리	A-15	주요정보통신기반시설의 서비스 현황을 식별하고 업무 절차와 흐름을 파악하여 문서화	상
	A-16	연 1회 이상 정기적으로 위험 평가 수행	상
	A-17	위험평가에 따른 연간 보호대책 이행계획 수립 및 경영진 보고	상
감사	A-18	법적 요구사항의 준수여부를 연 1회 이상 정기적 검토	상
	A-19	주기적으로 정보보호 감사 계획 수립·이행	상
	A-20	감사결과를 경영진에게 보고하여 적정한 사후관리를 시행	상
인적 보안	A-21	정보보호 관련 직무자의 책임과 역할을 명확히 정의하여 문서화	상
	A-22	기반시설 업무 담당자 지정 시 신원, 업무능력, 교육정도, 경력 등에 대한 적격심사 수행	상
	A-23	기반시설 업무 담당자 지정 시 보안 서약서나 비밀유지 확약서 작성	상

분류	번호	취약점 점검 항목	등급
	A-24	기반시설 업무 담당자 지정 해제 시 별도의 비밀유지 확약서 작성	상
	A-25	기반시설 업무 담당자 지정 해제 시 지체 없는 정보자산 반납, 접근권한 회수・조정, 결과 확인 등의 절차 수립・이행	상
	A-26	기반시설 업무 관련자가 정보보호 정책을 위반할 경우 이에 대한 징계와 관련된 사항을 규정에 명시	상
외부자 보안	A-27	외부 서비스 이용 및 업무 위탁에 따른 신규 외부자에 대한 보안 서약서 작성	상
	A-28	기반시설 범위 내에서 발생하고 있는 외부 서비스 이용 및 업무 위탁 현황을 식별 및 관리	상
	A-29	외부 서비스 이용 및 업무 위탁에 따른 정보보호 요구사항을 식별하고 이를 계약서 또는 협정서에 명시	상
	A-30	유지보수 등을 위한 외부자 임시 방문 시 정보 및 자산 접근에 대한 보안 규정 사전 고지	상
	A-31	외부자가 계약서, 협정서, 내부정책에 명시된 정보보호 요구사항을 준수하고 있는지 주기적으로 점검 또는 감사를 수행	상
	A-32	외부자의 보안 관련 사항 위반이나 침해사고 발생 시, 이에 따른 조치 수행	상
	A-33	외부자의 계약만료, 업무 종료, 담당자 변경 시 자산 반납, 접근권한 삭제 및 비밀유지 확약서 작성 등이 이루어질 수 있도록 보안대책 수립・이행	상
교육 및 훈련	A-34	정보보호 인식제고를 위한 교육 및 훈련 계획을 종합적으로 수립하여 정기적으로 실시	상
	A-35	전체 임직원 및 외부자에 대하여 정보보호 교육 및 훈련 수행	상
	A-36	교육 및 훈련은 대상자의 직위 및 업무 특성에 따라 차등화하여 실시	상
	A-37	교육 및 훈련의 효과가 측정・분석되어 차기 교육 및 훈련에 반영	상
	A-38	유관기관에서 공유한 보안공지・권고문 등에 대한 내용을 임직원 및 외부자에게 공유하고 조치요령을 안내	상
인증 및 권한 관리	A-39	담당 업무에 따라 시스템에 접근할 수 있는 사용자 계정 및 접근권한 부여 방법과 범위 등을 정의 및 이행	상
	A-40	내・외부에서 시스템 접근 시 안전한 인증 방법 및 절차를 마련하고 이에 따라 이행	상
	A-41	시스템에 대한 안전한 사용자 비밀번호 관리 절차 및 작성 규칙 수립・이행	상
	A-42	시스템에 대한 사용자 계정 및 접근권한의 적정성 검토 기준, 검토 주체, 검토 방법, 주기 등을 수립하여 이행	상
접근 통제	A-43	네트워크 접근통제 유지를 위해 접근권한 통제, 원격접속 관리, 네트워크 분리 등의 내용을 포함한 네트워크 운영 보안 정책을 수립・이행	상
	A-44	시스템의 목적 및 민감도 등에 따라 네트워크를 분리 운영하고 각 영역 간 접근통제를 적용	상
	A-45	접근통제 규칙은 관리자의 승인을 거쳐서 설정 또는 변경	상
	A-46	접근통제 정책의 적합성 여부에 대해 주기적 검토	상
	A-47	방화벽, 침입탐지시스템 구축 등 안전한 네트워크를 위한 대책을 마련	상

분류	번호	취약점 점검 항목	등급
	A-48	외부 네트워크를 통한 원격작업(재택근무, 장애대응 등)에 대한 책임자 승인, 작업내용 및 범위, 기간 설정, 접근 로그 기록/검토 등이 포함된 정책(절차) 수립・이행	상
	A-49	네트워크를 통해 시스템을 운영하는 경우 원칙적으로 시스템 관리는 내부의 특정 단말기에서만 할 수 있도록 제한	상
	A-50	외부에서 내부 시스템 접속 시 VPN 등 안전한 접속 수단 적용	상
	A-51	내부망(업무망)과 인터넷망을 분리하여 운용	상
	A-52	망분리 후 안전한 자료전송을 위한 시스템을 도입하여 사용	상
	A-53	인터넷 전화망과 일반 전산망은 분리하여 운용	상
	A-54	내부에 상주하는 외부자에 대하여 네트워크를 분리하여 운영	상
	A-55	무선네트워크 사용 시 상급기관장의 보안성 검토를 필하거나 안전한 암호화 알고리즘 및 암호키 설정 등의 적절한 보안조치를 적용	상
	A-56	인가된 임직원만이 인가된 단말을 이용하여 무선네트워크를 사용할 수 있도록 사용 신청 및 해지 절차를 수립・이행	상
	A-57	무선네트워크 무단 사용 여부, 비인가 무선 중계기(AP) 설치 여부, 우회 정보통신망 사용 차단 여부 등을 주기적으로 점검	상
운영 관리	A-58	자산 및 시스템을 신규 도입・개발 또는 변경하는 경우 법, 규제, 계약상의 요구사항을 정의하여 문서화	상
	A-59	자산 및 시스템을 신규 도입・개발 또는 변경하는 경우 보안성 검토 및 호환성 검토 수행하고 보안책임자는 이를 확인 및 승인	상
	A-60	시스템의 변경관리 절차 수립・이행	상
	A-61	정보보호시스템은 국내용 CC인증을 받았거나, 보안적합성 검증 수행	상
	A-62	제품 및 서비스에서 계약 등으로 협의된 사항 이외 이상행위가 발생하는지 모니터링	상
	A-63	개발 및 테스트 설비는 실제 운영 설비와 분리하여 운영	상
	A-64	개발자와 운영자의 접근 권한 분리	상
	A-65	업무용 시스템(ERP, 그룹웨어 등)의 소스코드 접근권한을 차등 부여하고 별도 저장장치에 보관	상
	A-66	업무용 시스템(ERP, 그룹웨어 등)의 소스코드 변경 시 보안약점 분석도구를 통해 취약점 점검	상
	A-67	주요 시스템 및 정보보호제품의 변경을 위한 공식적인 절차 수립・이행	상
	A-68	유지보수 작업 전 공식적인 작업 신청 및 수행절차를 수립・이행하고 작업 기록을 주기적으로 검토	상
	A-69	장애탐지, 장애기록, 장애분석, 장애복구, 장애보고 등의 사항을 포함하는 시스템의 장애관리 지침 문서화	상
	A-70	백업 대상, 주기, 방법, 보관 장소, 보관기간, 소산 등을 포함한 백업 절차 수립・이행	상

분류	번호	취약점 점검 항목	등급
	A-71	백업된 정보의 완전성과 정확성, 복구절차의 적절성을 확인하기 위하여 정기적으로 복구 테스트 수행	상
	A-72	전자기록 보관을 위한 별도의 방법(아카이빙)을 마련하고, 이를 통해 관리	상
	A-73	시스템 및 정보보호시스템에 대한 접근기록(로그 등)을 생성·보관하고, 이에 대한 비인가 열람, 훼손 등을 방지하기 위한 보호대책 운영	상
	A-74	시스템과 네트워크의 오류, 오·남용(비인가접속, 과다조회 등), 부정행위 등 이상징후를 인지할 수 있도록 로그 검토 주기, 대상, 방법 등을 포함한 로그 검토 및 모니터링 절차 수립·이행	상
	A-75	로그 및 모니터링 결과를 월 1회 이상 책임자에게 보고	상
	A-76	정보나 매체가 용도 폐기되기 위한 폐기 방법 수립·이행	상
	A-77	보안규정의 이행여부를 확인하는 주기적인 보안점검 및 불시 보안점검 수행	상
	A-78	비밀(대외비 포함)을 비밀관리기록부 등에 등재하여 관리	상
	A-79	출력된 비밀문서의 경우 잠금장치가 있는 캐비넷 등에 안전하게 보관	상
	A-80	비밀 등 중요정보의 안전한 처리를 위한 보호대책을 마련하거나 시스템을 도입하여 사용	상
	A-81	정보통신망 세부 구성현황(IP 정보 등)등을 비공개 이상으로 관리	상
	A-82	중요 데이터와 일반 데이터를 다른 서버에 분리 보관	상
	A-83	홈페이지 게시 자료에 대해 게시 절차를 마련하고 시행	상
	A-84	개인정보 및 주요정보의 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호강도, 암호사용, 암호키 관리 등이 포함된 암호정책 수립·이행	상
	A-85	암호키를 복구하기 위한 복구 절차를 수립하고 복구 내역 검토	상
보안 관리	A-86	침입차단 및 탐지 도구는 조직의 보안 정책과 규칙에 적합하게 설치하여 운영	상
	A-87	외부자와 정보 공유, 네트워크 공유 등에 따른 보안위협에 대한 대책 운영	상
	A-88	정보통신망에 비인가 PC, 노트북 등을 연결 시 차단 및 차단 이력 주기적 검토	상
	A-89	이동형 장치(노트북, 태블릿, 보조저장매체 등)의 사용 및 반출입에 대한 통제절차 수립·이행	상
	A-90	이동형 장치(노트북, 태블릿, 보조저장매체 등)의 반출입 시 통제 절차에 따른 기록 유지 관리하고 절차 준수여부를 확인할수 있도록 반출입 이력을 주기적으로 점검	상
	A-91	스마트폰·개인휴대단말기(태블릿)·전자제어장비 등 정보통신기기를 활용하는 경우, 업무자료 등 중요정보 보호 및 안전한 전송을 위한 방안 마련	상
	A-92	보조저장매체의 사용을 주기적으로 점검하고 운영 현황을 최신화	상
	A-93	노트북, 보조저장매체 등 이동형 장치의 분실을 통한 자료 유출 대비책 마련	상
	A-94	서버, 네트워크시스템, 보안시스템, PC 등 자산별 특성 및 중요도에 따라 운영체제(OS)와 소프트웨어의 패치관리 정책 및 절차 수립·이행	상

분류	번호	취약점 점검 항목	등급
	A-95	서버, 네트워크시스템, 보안시스템, PC 등의 운영체제, 소프트웨어 등이 개발사로부터 보안 지원이 되지 않을 경우 해당 제품을 교체하거나 보안대책 마련	상
	A-96	바이러스 등 악성프로그램을 대비한 보안프로그램의 설치·운영 등 보호대책 운영	상
	A-97	'사이버보안진단의 날' 등과 같이 월별 보안 중점점검사항에 대해 매월 보안점검 및 조치활동 수행	상
	A-98	네트워크, 메신저 등으로부터의 허가되지 않았거나 불분명한 파일의 다운로드를 금지하고, 부득이하게 다운로드 받을 경우 바이러스 검사 수행	상
	A-99	스팸 메일 수신을 줄이기 위한 방안(스팸차단 솔루션)을 마련	상
	A-100	개인정보의 유출 등을 방지하기 위해 접근 권한의 관리, 접근통제, 암호화, 접속기록의 보관 및 점검 등 개인정보의 안전성 확보에 필요한 조치 이행	상
	A-101	서비스 거부(DDoS) 공격 방지를 위한 대응방안(그린DDoSZone 등) 수립 및 운영	상
	A-102	주요정보통기반시설과 직·간접적으로 연계된 시스템을 대상으로 모의해킹 수행 및 보안대책 마련	상
	A-103	시스템 및 사용 장비에 대한 보안 취약점에 대한 주기적 검토 및 보완 프로세스 운영	상
사고 대응	A-104	침해사고 및 개인정보 유출사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차 수립	상
	A-105	침해사고 발생 시 신속한 보안사고 보고를 위한 절차를 문서화하고 있고 이에 따라 신속한 보고 수행	상
	A-106	침해사고 시 외부기관 및 전문가들과의 대응협조체계 구축	상
	A-107	사이버위기 '주의' 이상 경보 발령 및 피해발생 등 필요 시 대응할 수 있는 '긴급대응반'을 구성	상
	A-108	부정접근 사례나 보안사고 내역을 지속적으로 모니터링	상
	A-109	침해사고 발생에 대비한 대응절차 및 방법 숙지를 위한 주기적인 교육·훈련 실시	상
	A-110	보안사고 유형, 범위, 영향 등을 포함한 보안사고 분석 결과를 기록 및 관리	상
	A-111	보안 취약점 및 사고 발생 시 이에 대한 보완작업 절차 마련	상
	A-112	사이버침해사고 발생 후 재발방지 대책 수립·이행	상
	A-113	침해사고 처리, 계약증빙 및 소송 등을 위한 적정한 증거자료 확보에 관한 지침 수립·이행	상
업무 연속성	A-114	기반시설의 서비스(업무) 연속성을 위협할 수 있는 IT 재해 유형을 식별하고 유형별 피해규모 및 업무에 미치는 영향을 분석하여 핵심 IT 서비스(업무) 및 시스템을 식별	상
	A-115	핵심 IT서비스(업무) 및 시스템의 특성에 따른 복구 목표시간, 복구 목표시점을 정의	상
	A-116	재해 및 재난 발생 시에도 기반시설 서비스 및 시스템의 연속성을 보장할 수 있도록 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구 계획 수립·이행	상
	A-117	보안중요성이 높은 등급의 시스템들은 이중화하여 관리	상
	A-118	모의 훈련 등을 통해 업무 연속성을 지속적으로 검토 및 관리하고, 조직 내의 변경이 있을	상

분류	번호	취약점 점검 항목	등급
		경우 이에 대한 사항을 반영	

□ 물리적 분야

분류	번호	취약점 점검 항목	등급
물리 보안	P-1	보호구역의 출입에 관한 정책과 절차를 수립하고 이에 따라 출입통제 수행	상
	P-2	물리적 중요도에 따라 제한구역, 통제구역 등으로 분류하는 다단계 보호 대책 수행	상
	P-3	주요 시스템에 대한 별도의 출입통제를 실시하거나 이중의 보호장치 설치	상
	P-4	민감한 시설에 대해 물리적으로 접근하는 사람들의 출입기록 및 허가의 타당성을 주기적으로 검토	상
	P-5	제한구역 내 작업에 대한 추가적인 통제 수단 및 안내 지침 마련	상
	P-6	주요시설에 대한 출입기록은 출입일로부터 일정기간 이상 보관	상
	P-7	외부인에 대해서 출입증을 발급하고, 출입권한은 출입목적이 필요한 구역내로 한정	상
	P-8	전산 장비실에 외부협력업체 출입 시 내부 임직원이 상시 동행하는 등 통제방안 마련	상
	P-9	시각적으로 구분이 가능한 신분증 패용	상
	P-10	주요장비, 대체시스템 및 자료들을 화재, 습도 등의 환경재해로부터 보호되는 적절한 곳에 배치하여 보호	상
	P-11	전원 공급 이상이나 기타 전기 관련 사고로부터 장비 보호(UPS, 비상발전기, 이중전원선 등의 설비)	상
	P-12	전원 공급 이상이나 기타 전기 관련 사고로부터 장비를 보호하기 위해 설비 상태에 대해 정기적으로 검토	상
	P-13	전원선 및 통신선은 도청이나 손상으로부터 보호	상
	P-14	누전이 발생하였을 때 이를 차단할 수 있도록 누전차단기 또는 누전경보기의 설치	상
	P-15	전산실에 24시간 항온, 항습을 유지하기 위하여 온습도 측정이 가능하도록 항온항습기 등을 설치 및 운영	상
	P-16	주요시설(중앙감시실, 전산실, 전력관련시설, 통신장비실, 방재센터 등)에는 기존 조명설비의 작동이 멈추는 경우에도 작업이 가능하도록 비상조명을 설치	상
	P-17	주요시설의 출입구와 전산실 및 통신장비실 내부에 CCTV를 설치	상
	P-18	CCTV 운용 시 중계・관제서버, 관리용 PC, 정보통신망 등에 대해 보안대책을 수립	상

□ 기술적 분야

가. 유닉스

분류	번호	취약점 점검 항목	등급
계정 관리	U-1	root 계정 원격 접속 제한	상
	U-2	비밀번호 관리정책 설정	상
	U-3	계정 잠금 임계값 설정	상
	U-4	비밀번호 파일 보호	상
	U-5	root 이외의 UID가 '0' 금지	상
	U-6	사용자 계정 su 기능 제한	상
	U-7	불필요한 계정 제거	하
	U-8	관리자 그룹에 최소한의 계정 포함	중
	U-9	계정이 존재하지 않는 GID 금지	하
	U-10	동일한 UID 금지	중
	U-11	사용자 shell 점검	하
	U-12	세션 종료 시간 설정	하
	U-13	안전한 비밀번호 암호화 알고리즘 사용	중
파일 및 디렉토리	U-14	root 홈, 패스 디렉터리 권한 및 패스 설정	상
	U-15	파일 및 디렉터리 소유자 설정	상
	U-16	/etc/passwd 파일 소유자 및 권한 설정	상
	U-17	시스템 시작 스크립트 권한 설정	상
	U-18	/etc/shadow 파일 소유자 및 권한 설정	상
	U-19	/etc/hosts 파일 소유자 및 권한 설정	상
	U-20	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상
	U-21	/etc/(r)syslog.conf 파일 소유자 및 권한 설정	상
	U-22	/etc/services 파일 소유자 및 권한 설정	상
	U-23	SUID, SGID, Sticky bit 설정 파일 점검	상
	U-24	사용자, 시스템 환경변수 파일 소유자 및 권한 설정	상
	U-25	world writable 파일 점검	상

분류	번호	취약점 점검 항목	등급
	U-26	/dev에 존재하지 않는 device 파일 점검	상
	U-27	$HOME/.rhosts, hosts.equiv 사용 금지	상
	U-28	접속 IP 및 포트 제한	상
	U-29	hosts.lpd 파일 소유자 및 권한 설정	하
	U-30	UMASK 설정 관리	중
	U-31	홈디렉토리 소유자 및 권한 설정	중
	U-32	홈디렉토리로 지정한 디렉토리의 존재 관리	중
	U-33	숨겨진 파일 및 디렉토리 검색 및 제거	하
서비스 관리	U-34	Finger 서비스 비활성화	상
	U-35	공유 서비스에 대한 익명 접근 제한 설정	상
	U-36	r 계열 서비스 비활성화	상
	U-37	crontab 설정파일 권한 설정 미흡	상
	U-38	DoS 공격에 취약한 서비스 비활성화	상
	U-39	불필요한 NFS 서비스 비활성화	상
	U-40	NFS 접근 통제	상
	U-41	불필요한 automountd 제거	상
	U-42	불필요한 RPC 서비스 비활성화	상
	U-43	NIS, NIS+ 점검	상
	U-44	tftp, talk 서비스 비활성화	상
	U-45	메일 서비스 버전 점검	상
	U-46	일반 사용자의 메일 서비스 실행 방지	상
	U-47	스팸 메일 릴레이 제한	상
	U-48	expn, vrfy 명령어 제한	중
	U-49	DNS 보안 버전 패치	상
	U-50	DNS ZoneTransfer 설정	상
	U-51	DNS 서비스의 취약한 동적 업데이트 설정 금지	중
	U-52	Telnet 서비스 비활성화	중

분류	번호	취약점 점검 항목	등급
	U-53	FTP 서비스 정보 노출 제한	하
	U-54	암호화 되지 않는 FTP 서비스 비활성화	중
	U-55	ftp 계정 shell 제한	중
	U-56	FTP 서비스 접근 제어 설정	하
	U-57	Ftpusers 파일 설정	중
	U-58	불필요한 SNMP 서비스 구동 점검	중
	U-59	안전한 SNMP 버전 사용	상
	U-60	SNMP Community String 복잡성 설정	중
	U-61	SNMP Access Control 설정	상
	U-62	로그인 시 경고 메시지 설정	하
	U-63	sudo 명령어 접근 관리	중
패치 관리	U-64	주기적 보안 패치 및 벤더 권고사항 적용	상
로그 관리	U-65	NTP 및 시각 동기화 설정	중
	U-66	정책에 따른 시스템 로깅 설정	중
	U-67	로그 디렉터리 소유자 및 권한 설정	중

나. 윈도우즈

분류	번호	취약점 점검 항목	등급
계정 관리	W-01	Administrator 계정 이름 변경 등 보안성 강화	상
	W-02	Guest 계정 비활성화	상
	W-03	불필요한 계정 제거	상
	W-04	계정 잠금 임계값 설정	상
	W-05	해독 가능한 암호화를 사용하여 암호 저장 해제	상

분류	번호	취약점 점검 항목	등급
	W-06	관리자 그룹에 최소한의 사용자 포함	상
	W-07	Everyone 사용 권한을 익명 사용자에게 적용	중
	W-08	계정 잠금 기간 설정	중
	W-09	비밀번호 관리정책 설정	상
	W-10	마지막 사용자 이름 표시 안 함	중
	W-11	로컬 로그온 허용	중
	W-12	익명 SID/이름 변환 허용 해제	중
	W-13	콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한	중
	W-14	원격터미널 접속 가능한 사용자 그룹 제한	중
서비스 관리	W-15	사용자 개인키 사용 시 암호 입력	상
	W-16	공유 권한 및 사용자 그룹 설정	상
	W-17	하드디스크 기본 공유 제거	상
	W-18	불필요한 서비스 제거	상
	W-19	불필요한 IIS 서비스 구동 점검	상
	W-20	NetBIOS 바인딩 서비스 구동 점검	상
	W-21	암호화되지 않는 FTP 서비스 비활성화	상
	W-22	FTP 디렉토리 접근권한 설정	상
	W-23	공유 서비스에 대한 익명 접근 제한 설정	상
	W-24	FTP 접근 제어 설정	상
	W-25	DNS Zone Transfer 설정	상
	W-26	RDS(Remote Data Services)제거	상
	W-27	최신 Windows OS Build 버전 적용	상
	W-28	터미널 서비스 암호화 수준 설정	중
	W-29	불필요한 SNMP 서비스 구동 점검	중
	W-30	SNMP Community String 복잡성 설정	중
	W-31	SNMP Access Control 설정	중
	W-32	DNS 서비스 구동 점검	중

분류	번호	취약점 점검 항목	등급
	W-33	HTTP/FTP/SMTP 배너 차단	하
	W-34	Telnet 서비스 비활성화	중
	W-35	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거	중
	W-36	원격터미널 접속 타임아웃 설정	중
	W-37	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검	중
패치 관리	W-38	주기적 보안 패치 및 벤더 권고사항 적용	상
	W-39	백신 프로그램 업데이트	상
로그 관리	W-40	정책에 따른 시스템 로깅 설정	중
	W-41	NTP 및 시각 동기화 설정	중
	W-42	이벤트 로그 관리 설정	하
	W-43	이벤트 로그 파일 접근 통제 설정	중
보안 관리	W-44	원격으로 액세스할 수 있는 레지스트리 경로	상
	W-45	백신 프로그램 설치	상
	W-46	SAM 파일 접근 통제 설정	상
	W-47	화면보호기 설정	하
	W-48	로그온하지 않고 시스템 종료 허용	상
	W-49	원격 시스템에서 강제로 시스템 종료	상
	W-50	보안 감사를 로그할 수 없는 경우 즉시 시스템 종료	상
	W-51	SAM 계정과 공유의 익명 열거 허용 안 함	상
	W-52	Autologon 기능 제어	상
	W-53	이동식 미디어 포맷 및 꺼내기 허용	상
	W-54	Dos공격 방어 레지스트리 설정	중
	W-55	사용자가 프린터 드라이버를 설치할 수 없게 함	중
	W-56	SMB 세션 중단 관리 설정	중
	W-57	로그온 시 경고 메시지 설정	하
	W-58	사용자별 홈 디렉터리 권한 설정	중
	W-59	LAN Manager 인증 수준	중

분류	번호	취약점 점검 항목	등급
	W-60	보안 채널 데이터 디지털 암호화 또는 서명	중
	W-61	파일 및 디렉토리 보호	중
	W-62	시작프로그램 목록 분석	중
	W-63	도메인 컨트롤러-사용자의 시간 동기화	중
	W-64	윈도우 방화벽 설정	중

다. 웹 서비스

분류	번호	취약점 점검 항목	등급
계정 관리	WEB-01	Default 관리자 계정명 변경	상
	WEB-02	취약한 비밀번호 사용 제한	상
	WEB-03	비밀번호 파일 권한 관리	상
서비스 관리	WEB-04	웹 서비스 디렉터리 리스팅 방지 설정	상
	WEB-05	지정하지 않은 CGI/ISAPI 실행 제한	상
	WEB-06	웹 서비스 상위 디렉터리 접근 제한 설정	상
	WEB-07	웹 서비스 경로 내 불필요한 파일 제거	중
	WEB-08	웹 서비스 파일 업로드 및 다운로드 용량 제한	하
	WEB-09	웹 서비스 프로세스 권한 제한	상
	WEB-10	불필요한 프록시 설정 제한	상
	WEB-11	웹 서비스 경로 설정	중
	WEB-12	웹 서비스 링크 사용 금지	중
	WEB-13	웹 서비스 설정 파일 노출 제한	상
	WEB-14	웹 서비스 경로 내 파일의 접근 통제	상
	WEB-15	웹 서비스의 불필요한 스크립트 매핑 제거	상
	WEB-16	웹 서비스 헤더 정보 노출 제한	중
	WEB-17	웹 서비스 가상 디렉토리 삭제	중
	WEB-18	웹 서비스 WebDAV 비활성화	상
보안 설정	WEB-19	웹 서비스 SSI(Server Side Includes) 사용 제한	중

분류	번호	취약점 점검 항목	등급
	WEB-20	SSL/TLS 활성화	상
	WEB-21	HTTP 리디렉션	중
	WEB-22	에러 페이지 관리	하
	WEB-23	LDAP 알고리즘 적절하게 구성	중
패치 및 로그관리	WEB-24	별도의 업로드 경로 사용 및 권한 설정	중
	WEB-25	주기적 보안 패치 및 벤더 권고사항 적용	상
	WEB-26	로그 디렉터리 및 파일 권한 설정	중

라. 보안 장비

분류	번호	취약점 점검 항목	등급
계정 관리	S-01	보안장비 Default 계정 변경	상
	S-02	비밀번호 관리정책 설정	상
	S-03	보안장비 계정별 권한 설정	상
	S-04	보안장비 계정 관리	상
	S-05	계정 잠금 임계값 설정	상
접근 관리	S-06	보안장비 원격 관리 접근 통제	상
	S-07	보안장비 보안 접속	상
	S-08	세션 종료 시간 설정	상
패치 관리	S-09	주기적 보안 패치 및 벤더 권고사항 적용	상
로그 관리	S-10	보안장비 로그 설정	중
	S-11	보안장비 로그 보관	중
	S-12	보안장비 정책 백업 설정	중
	S-13	원격 로그 서버 사용	중
	S-14	NTP 및 시각 동기화 설정	중
기능 관리	S-15	정책 관리	상
	S-16	NAT 설정	상
	S-17	DMZ 설정	상
	S-18	최소한의 서비스만 제공	상
	S-19	이상징후 탐지 모니터링 수행	상

	S-20	장비 사용량 검토	상
	S-21	SNMP 서비스 확인	상
	S-22	SNMP Community String 복잡성 설정	상
	S-23	유해 트래픽 탐지/차단 정책 설정	중

마. 네트워크 장비

분류	번호	취약점 점검 항목	등급
계정 관리	N-01	비밀번호 설정	상
	N-02	비밀번호 복잡성 설정	상
	N-03	암호화된 비밀번호 가용	상
	N-04	계정 잠금 임계값 설정	상
	N-05	사용자, 명령어별 권한 수준 설정	중
접근 관리	N-06	VTY 접근(ACL) 설정	상
	N-07	세션 종료 시간 설정	상
	N-08	VTY 접속 시 안전한 프로토콜 사용	중
	N-09	불필요한 보조 입출력 포트 사용 금지	중
	N-10	로그인 시 경고 메시지 설정	중
	N-11	원격 로그서버 사용	중
패치 관리	N-12	주기적 보안 패치 및 벤더 권고사항 적용	상
로그 관리	N-13	로깅 버퍼 크기 설정	중
	N-14	정책에 따른 로깅 설정	중
	N-15	NTP 및 시각 동기화 설정	중
	N-16	Timestamp 로그 설정	하
기능 관리	N-17	SNMP 서비스 확인	상
	N-18	SNMP Community String 복잡성 설정	상
	N-19	SNMP ACL 설정	상
	N-20	SNMP Community 권한 설정	상
	N-21	TFTP 서비스 차단	상
	N-22	Spoofing 방지 필터링 적용	상

분류	번호	취약점 점검 항목	등급
	N-23	DDoS 공격 방어 설정 또는 DDoS 장비 사용	상
	N-24	사용하지 않는 인터페이스 비활성화	상
	N-25	TCP keepalive 서비스 설정	중
	N-26	Finger 서비스 차단	중
	N-27	웹 서비스 차단	중
	N-28	TCP/UDP small 서비스 차단	중
	N-29	Bootp 서비스 차단	중
	N-30	CDP 서비스 차단	중
	N-31	Directed-broadcast 차단	중
	N-32	Source 라우팅 차단	중
	N-33	Proxy ARP 차단	중
	N-34	ICMP unreachable, Redirect 차단	중
	N-35	identd 서비스 차단	중
	N-36	Domain lookup 차단	중
	N-37	pad 차단	중
	N-38	mask-reply 차단	중

바. 제어시스템

분류	번호	취약점 점검 항목	등급
계정 관리	C-01	계정기능이 있는 제어시스템 구성요소에 대해 계정을 안전하게 설정하여 사용	상
	C-02	제어시스템 계정의 로그인/로그아웃, 사용명령 등 사용기록을 저장	상
	C-03	제어시스템 계정입력 시 비밀번호 마스킹 처리, 입력값 에러 발생 시 제공 정보 제한 수행	상
	C-04	제어시스템 계정을 관리, 운영, 유지보수 등 용도에 따라 분리하고 운용	중
	C-05	제어시스템 계정에 대해 관리, 운영, 유지보수 등 용도에 맞는 최소 권한 부여	중
	C-06	제어시스템 운전원 별 유일 계정 부여 또는 시간별 사용자 기록 유지	중
서비스 관리	C-07	제어시스템 구성요소에 대한 시각 동기화 수행	상
	C-08	제어시스템에 불필요한 서비스 및 취약한 서비스 제거 또는 보완대책 수행	상
	C-09	제어시스템 구성요소에 대한 관리자 페이지 운영 시 이에 대한 접근통제(사전인가 접근만 허용) 수행	중
	C-10	제어시스템 내 파일/디렉토리 접근권한 및 신뢰관계를 적절히 부여	중

	C-11	제어시스템 내 제어와 직접적인 관련이 없는 불필요 프로그램 삭제	중
	C-12	제어시스템 운영 정보, 제어명령 등 중요정보에 대한 위변조 및 replay 공격 방지 대책 적용	중
	C-13	제어시스템 내 전달되는 제어명령 및 파라미터의 정상 범위를 식별하고 관리	하
	C-14	제어시스템 내 사용자 통신세션에 대해 세션타임아웃 적용	하
	C-15	GPS 스푸핑/재밍 공격 등 시각동기화 서비스를 교란하기 위한 공격에 대비한 보안조치 수행	하
패치 관리	C-16	제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 제조사 협력방안, 테스트 방안 등의 절차 수립	상
	C-17	외부 업체, 인터넷을 통한 다운로드 등의 경로로 반입된 각종 패치·업데이트 파일에 대해 무결성 검증 및 클린 PC를 통한 악성코드 존재 여부 검사 수행	상
	C-18	제어시스템 구성요소의 알려진 취약점에 대해 보안패치 적용 또는 상응하는 대응책 적용	상
	C-19	운영체제, 응용프로그램, 펌웨어 등에 대해 안정성이 확인된 최신버전의 소프트웨어 사용 및 기술지원이 종료된 제품 미사용	중
	C-20	제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경을 구축	하
네트워크 접근통제	C-21	제어 네트워크는 업무망, 인터넷, CCTV망 등 외부망과 물리적으로 분리하여 사용	상
	C-22	제어 네트워크 외부로 자료전달 시 물리적 일방향 자료전달 환경을 구축하여 외부에서 제어 네트워크로의 침입을 차단	상
	C-23	제어 네트워크에 무선인터넷, 테더링, 외부 유선망 등의 외부망 연결을 제한하고 주기적으로 점검	상
	C-24	제어 네트워크에 비인가된 시스템/기기에 대한 연결 및 접속을 차단	상
	C-25	물리적 일방향 자료전달 환경의 올바른 동작 및 운용에 대한 주기적인 점검 수행	상
	C-26	제어 네트워크를 용도에 따라 세분화하고, 접근제어를 수행하여 제어시스템 운영에 필요한 네트워크, 시스템 간의 통신만 허용	하
물리적 접근통제	C-27	제어시스템에 대해 네트워크 포트, USB 포트 등 외부 연결 접점에 대해 허가받은 사항을 제외하고 모두 물리적 또는 논리적으로 차단	상
	C-28	제어시스템 구성요소를 물리적으로 보호할 수 있는 조치 적용(잠금장치가 있는 함체, 랙, 수납책상 등)	중
보안위협 탐지	C-29	백신 프로그램 설치가 가능한 제어시스템 구성요소에 대해 악성코드 감염 및 차단을 위한 백신 프로그램 설치	상
	C-30	이상 트래픽 발생 탐지 등 제어시스템 내의 보안 관리를 위해 적합한 침입탐지시스템 등을 구축 및 운용하고, 구축된 보안 솔루션 및 보안장비에서 탐지한 보안 이벤트에 대해 모니터링 수행	하
복구 대응	C-31	제어시스템 대상 사이버 위기대응 매뉴얼을 수립	상
	C-32	제어시스템 대상 사이버 위기대응 훈련을 정기적으로 시행	상
	C-33	제어시스템 침해사고 대응을 위한 제어시스템 설정, 중요 데이터 등을 백업 및 관리	상
	C-34	제어시스템의 장애발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 수립	중

	C-35	제어시스템의 장애발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 훈련을 정기적으로 시행	중
	C-36	제어시스템 조작불능에 대비하여 수작업 운전 매뉴얼 작성 및 교육훈련 시행	중
	C-37	제어시스템의 각종 이벤트에 대한 로그를 관리하기 위한 중앙집중식 로그 관리 수행	하
	C-38	제어시스템 구성요소의 기준 형상을 설정하고 변경 및 업데이트 시 형상관리 수행	하
	C-39	제어시스템 주요 장비 및 제어 네트워크 장비에 대해 이중화	하
	C-40	제어시스템 보호를 위한 화재탐지 설비 및 화재 진압설비를 구비	하
	C-41	제어시스템 보호를 위한 누수탐지 설비 및 침수 대응 장비 구비	하
	C-42	제어시스템에 대하여 정기적으로 사이버 위험 시나리오를 식별하고, 완화 방안 수립	하
보안 관리	C-43	제어시스템 구성요소에 대한 자산정보(담당자, 펌웨어 버전, 설치 SW 등)를 항상 최신으로 유지관리	상
	C-44	제어시스템 중요 구성요소가 설치된 장소를 보호구역으로 설정	상
	C-45	제어시스템에서 USB 등 이동형 저장매체를 사용해야 하는 경우, 사전정의된 정책에 따라 사용	상
	C-46	제어 네트워크에 연결되는 외부 정보통신기기 반출입시 클린존 통과, 관리대장 작성 등 관리절차 마련	상
	C-47	제어시스템의 특성을 반영한 정보보안 정책, 지침을 수립	중
	C-48	제어시스템 운영업무에 대해 표준업무절차서를 작성하고 적용	중
	C-49	제어시스템 유지보수를 위한 전용 장비(노트북 등)를 마련하고 관련 정책을 시행	하
	C-50	허가에 의한 로직 변경 정책 수립	상
교육 훈련	C-51	제어시스템 운전원, 관리자, 유지보수인력, 보안인력에 대해 각 직무별 직무교육을 정기적으로 실시	하

사. PC

분류	번호	취약점 점검 항목	등급
계정 관리	PC-01	비밀번호의 주기적 변경	상
	PC-02	비밀번호 관리정책 설정	상
	PC-03	복구 콘솔에서 자동 로그온을 금지하도록 설정	중
서비스 관리	PC-04	공유 폴더 제거	상
	PC-05	항목의 불필요한 서비스 제거	상

	PC-06	비인가 상용 메신저 사용 금지	상
	PC-07	파일 시스템이 NTFS 포맷으로 설정	중
	PC-08	대상 시스템이 Windows 서버를 제외한 다른 OS로 멀티 부팅이 가능하지 않도록 설정	중
	PC-09	브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제하도록 설정	하
패치 관리	PC-10	주기적 보안 패치 및 벤더 권고사항 적용	상
	PC-11	지원이 종료되지 않은 Windows OS Build 적용	상
보안 관리	PC-12	Windows 자동 로그인 점검	중
	PC-13	바이러스 백신 프로그램 설치 및 주기적 업데이트	상
	PC-14	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상
	PC-15	OS에서 제공하는 침입차단 기능 활성화	상
	PC-16	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상
	PC-17	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안대책 수립	상
	PC-18	원격 지원을 금지하도록 정책을 설정	중

아. 데이터베이스

분류	번호	취약점 점검 항목	등급
계정 관리	D-01	기본 계정의 비밀번호, 정책 등을 변경하여 사용	상
	D-02	데이터베이스의 불필요 계정을 제거하거나, 잠금설정 후 사용	상
	D-03	비밀번호의 사용기간 및 복잡도를 기관의 정책에 맞도록 설정	상
	D-04	데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 대해서만 허용	상
	D-05	비밀번호 재사용에 대한 제약 설정	중
	D-06	DB 사용자 계정을 개별적으로 부여하여 사용	중
	D-07	root 권한으로 서비스 구동 제한	중
	D-08	안전한 암호화 알고리즘 사용	상
	D-09	일정 횟수의 로그인 실패 시 이에 대한 잠금정책 설정	중
접근 관리	D-10	원격에서 DB 서버로의 접속 제한	상
	D-11	DBA이외의 인가되지 않은 사용자가 시스템 테이블에 접근할 수 없도록 설정	상

분류	번호	취약점 점검 항목	등급
	D-12	안전한 리스너 비밀번호 설정 및 사용	상
	D-13	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브를 제거하여 사용	중
	D-14	데이터베이스의 주요 설정파일, 비밀번호 파일 등과 같은 주요 파일들의 접근 권한이 적절하게 설정	중
	D-15	관리자 이외의 사용자가 오라클 리스너의 접속을 통해 리스너 로그 및 trace 파일에 대한 변경 제한	하
	D-16	Windows 인증 모드 사용	하
옵션 관리	D-17	Audit Table은 데이터베이스 관리자 계정에 접근하도록 제한	하
	D-18	응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되지 않도록 조정	상
	D-19	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정	상
	D-20	인가되지 않은 Object Owner의 제한	하
	D-21	인가되지 않은 GRANT OPTION 사용 제한	중
	D-22	데이터베이스의 자원 제한 기능을 TRUE로 설정	하
	D-23	xp_cmdshell 사용 제한	상
	D-24	Registry Procedure 권한 제한	상
패치 관리	D-25	주기적 보안 패치 및 벤더 권고사항 적용	상
	D-26	데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정	상

자. 이동통신

분류	번호	취약점 점검 항목	등급
운영 관리	M-1	이동통신망 엣지 네트워크 운영 시 인터넷 연결 등을 고려한 보안기술을 적용	상
	M-2	이동통신망에서 가상화 기술 적용 시 계정관리, 이상징후 탐지 등 보안 설정 또는 기술 적용	상
	M-3	이동통신망 장비 및 SW 제조사 등과 보안정책을 마련하여 운영	상
	M-4	이동통신망 장비 구축과 네트워크 설계 시 보안 내재화를 수행	상

차. 웹(Web)

코드	취약점명	설 명	등급
CI	코드 인젝션	웹 애플리케이션 내 다양한 인젝션 공격(운영체제 명령 실행, LDAP, SSI, XPath, XML, SSTI 등)에 대해 사용자의 입력 값이 쿼리나 명령어로 삽입되어 비인가된 접근이나 코드 실행이 가능한 취약점	상
SI	SQL 인젝션	사용자 입력 값이 SQL 쿼리에 삽입되어 데이터베이스에 비인가된 접근 허용, 민감 데이터 조회, 수정, 삭제 등의 행위가 가능한 취약점	상
DI	디렉토리 인덱싱	브라우저를 통해 특정 디렉터리 내 파일 리스트가 노출되어 응용 시스템의 구조가 외부에 공개될 수 있으며, 민감한 정보가 포함된 설정 파일이 노출될 경우 2차 공격에 대한 정보를 제공할 수 있는 취약점	상
EP	에러페이지 적용 미흡	기본 에러페이지 설정 및 예외 처리가 미흡하여 웹서버 및 응용 시스템 정보, 스택 트레이스, 데이터베이스 쿼리 등 민감한 정보가 노출되어 공격 포인트로 악용될 가능성을 제공하는 취약점	상
IL	정보 누출	패킷이나 홈페이지 내 중요 정보(개인정보, 금융정보 등)가 노출될 경우 개인정보 유출로 인한 사생활 침해, 신원 도용, 피싱 공격 등의 위협이 발생할 수 있으며, 서버나 WAS의 초기 샘플 페이지, 백업 파일, 압축 파일 등이 노출될 경우 공격자가 시스템 구조를 파악하고 보안 설정 및 접근 제어 정책을 유출하여 2차 공격에 대한 정보를 제공할 수 있는 취약점	상
XS	크로스사이트 스크립트	웹애플리케이션을 사용해서 다른 최종 사용자의 클라이언트에서 임의의 스크립트가 실행되는 취약점	상
CF	크로스사이트 요청 위조(CSRF)	로그인한 사용자 브라우저로 하여금 사용자의 세션 쿠키와 기타 인증 정보를 포함하는 위조된 HTTP 요청을 취약한 웹애플리케이션에 전송하는 취약점	상
SF	서버사이드 요청 위조(SSRF)	서버 간 통신 시 입력값에 대한 검증이 미흡하여 외부에서 접근이 제한된 내부 서버 자원에 대한 정보 수집, 중요 정보(개인정보, 금융정보, 인사 정보 등) 탈취, 임의 명령 실행, 클라우드 환경 내 메타데이터 수집을 통한 네트워크 인프라 점유가 가능한 취약점	상
BF	약한 비밀번호 정책	비밀번호 복잡도 정책이 미흡하여 취약한 비밀번호로 회원가입이 가능할 경우 주변 정보를 토대로 작성한 사전대입공격 또는 무작위 공격으로 인한 계정 탈취의 가능성이 존재하는 취약점	상
IA	불충분한 인증 절차	사용자의 인증이 요구되는 페이지 및 프로세스(개인정보수정, 본인인증, OTP 인증 등)에 대한 인증 절차가 미흡할 경우 악의적인 접근으로 인해 중요정보가 유출 또는 변조될 가능성이 존재하는 취약점	상
IN	불충분한 권한 검증	사용자 식별 정보 또는 패킷 변조, Client 구간에서의 로직 변조 등의 데이터 변조를 통해 타 사용자의 권한 탈취, 부여되지 않은 권한 획득으로 인한 데이터 조작이 가능한 취약점	상
PR	취약한 비밀번호 복구 절차	취약한 비밀번호 복구 로직으로 인해 공격자가 불법적으로 다른 사용자의 비밀번호를 획득하거나 변경이 가능한 취약점	상
PV	프로세스 검증 누락	특정 의도된 기능들이 논리적 결함이나 다양한 요인으로 인해 오작동(가격변조, URL 직접 접근 등)하거나 프로세스 상 필수적인 단계를 생략하는 등의 행위가 가능한 취약점	상

코드	취약점명	설 명	등급
FU	악성 파일 업로드	파일 업로드 기능을 이용하여 악성 프로그램이나 시스템 명령어를 실행할 수 있는 웹 프로그램을 업로드 할 수 있는 취약점	상
FD	파일 다운로드	파일 다운로드 기능을 이용하여 주요 시스템 및 소스코드 파일을 다운로드 할 수 있는 취약점	상
IS	불충분한 세션 관리	사용자에게 발급되는 세션이 만료되지 않거나, 고정 및 예측 가능한 형태일 경우, 해당 세션을 탈취하여 타 사용자나 시스템에 무단 접근할 수 있으며, 이로 인해 중요 데이터의 무결성 훼손이 발생할 수 있는 취약점	상
SN	데이터 평문 전송	서버와 클라이언트간 통신 시 암호화하여 전송을 하지 않아 중요 정보 등이 평문으로 전송되는 취약점	상
CC	쿠키 변조	쿠키 검증이 미흡하여 쿠키 인젝션 등과 같은 쿠키 값 변조의 방법으로 다른 사용자로 위장하거나 권한 상승이 가능한 취약점	상
AE	관리자 페이지 노출	단순한 관리자 페이지 이름(admin, manager 등)이나 설정, 프로그램 설계상의 오류로 인해 관리자 메뉴에 직접 접근할 수 있는 취약점	상
AU	자동화 공격	웹 애플리케이션의 정해진 프로세스에 자동화된 공격을 수행함으로써 과부하 공격으로 인한 리소스 고갈, 정보 추출, 계정 정보 획득 등의 공격이 가능한 취약점	상
WM	불필요한 Method 사용	일반적인 환경에서 불필요한 메소드인 PUT, DELETE, TRACE 등의 메소드가 허용되어 서버 무결성 침해, 악성코드 삽입 등의 공격이 가능한 취약점	상

카. 가상화 장비

분류	번호	취약점 점검 항목	등급
계정 관리	HV-01	계정 로그오프/세션 관리	상
	HV-02	가상화 장비 외부접속 차단	상
	HV-03	가상화 장비 루트계정 관리	상
	HV-04	가상화 장비 계정 권한 관리	상
	HV-05	가상화 장비 사용자 인증 강화	상
	HV-06	비밀번호 관리정책 설정	상
	HV-07	계정 잠금 임계값 설정	상
시스템 서비스 관리	HV-08	시스템 사용 주의사항 출력 설정	중
	HV-09	NTP 및 시각 동기화 설정	중
	HV-10	SNMP Community String 복잡성 적용	중
	HV-11	MOB(Managed Object Browser) 서비스 비활성화	상

	HV-12	ESXi Shell 비활성화	상
	HV-13	ESXi Shell 세션 종료 시간 설정	상
	HV-14	원격 로그 서버 이용	중
	HV-15	시스템 주요 이벤트 로그 설정	상
	HV-16	비휘발성 경로 내 로그 파일 저장	상
가상머신 관리	HV-17	코어덤프 수집 기능 활성화	상
	HV-18	가상머신의 장치 변경 제한 설정	상
	HV-19	가상머신의 불필요한 장치 제거	상
	HV-20	가상머신 콘솔 클립보드 복사&붙여넣기 기능 비활성화	상
	HV-21	가상머신 콘솔 드래그 앤 드롭 기능 비활성화	상
가상 네트워크 관리	HV-22	가상스위치 MAC 주소 변경 정책 비활성화	상
	HV-23	가상스위치 무차별(Promiscuous) 모드 정책 비활성화	상
	HV-24	가상스위치 위조전송(Forged Transmits) 모드 정책 비활성화	상
	HV-25	주기적 보안 패치 및 벤더 권고사항 적용	상

타. 클라우드

분류	번호	취약점 점검 항목	등급
계정 관리	CA-01	사용자 계정 관리	상
	CA-02	사용자 정책 관리	중
	CA-03	MFA(Multi-Factor Authentication) 설정	상
	CA-04	클라우드 계정 비밀번호 정책 관리	중
권한 관리	CA-05	인스턴스 서비스 정책 관리	상
	CA-06	네트워크 서비스 정책 관리	상
가상 리소스 관리	CA-07	VPC 네트워크 서브넷 관리	상
	CA-08	가상 네트워크 리소스 관리	중
	CA-09	접근 제어 설정 관리	상
	CA-10	스토리지 리소스 퍼블릭 접근 관리	중
운영	CA-11	관계형 데이터베이스 암호화 설정	중

관리	CA-12	통신구간 암호화 설정	중
	CA-13	클라우드 서비스 사용자 계정 로깅 설정	상
	CA-14	인스턴스 로깅 설정	중
	CA-15	관계형 데이터베이스로깅 설정	중
	CA-16	오브젝트 스토리지 버킷 로깅 설정	중
	CA-17	로그 보관 기간 설정	중
	CA-18	백업 사용 여부	중
	CA-19	가상 리소스 이상징후 알림 설정	중