KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 018

October 2019

한국선급 활동

- IALA ENAV 위원회에서 해상 사이버보안 관련 표준화 활동
- TRIPARTITE 2019, 해사 사이버보안 동향 모니터링

[기획시리즈] ③ LTE 구조와 5G 분산형 네트워크 구조 비교

사이버 위협의 이해(OWASP Top 10)

KR 해상 사이버보안 형식승인 지침의 이해

용어 설명

IALA ENAV 위원회에서 사이버보안 의제 발표

한국선급은 10월 7일~11일 프랑스 파리에서 개최된 제 24차 IALA(국제항로표지협회) ENAV 위원회의 해상 사이버보안 표준화 회의에 참석하였다. IALA는 국제 해사업계에서 e-Navigation과 디지털 해상통신의 표준화를 주도하고 있는 국제기구이다. IMO, BIMCO, CIRM 등 국제 해사업계에서 최근 대두되고 있는 디지털 기술로 인해 사이버 위협에 노출될 가능성이 높아짐에 따라, IALA에서도 AtoN(항로표지), VTS(해상교통관제센터)에 사이버 보안 적용을 위한 표준화 논의를 중요한 이슈로 부각되고 있다. 이번 IALA ENAV 24 회의에서는 IALA 차원의 사이버보안 지침/권고서 개발 계획이 발표되었다. 한국선급은 IALA의 사이버보안 표준화 논의에 참여하여 한국선급이 개발한 형식승인 지침과 실제 적용 사례를 발표하였고, IALA ENAV 위원회에 참여하는 많은 정부대표와 산업계 회원사들로 부터 지속적인 협력을 요청받았다.

한국선급이 개발한 형식승인 지침은 국제표준(IEC 62443 4-2 및 IEC 61162-460 등)을 기반으로 사이버보안 형식승인 서비스를 시행하고 있으며, 현대중공업에서 개발한 최첨단 선박용 스마트 통합 통신장비인 HYUNDAI-ISCS에 사이버보안 형식승인 증서를 수여한바 있다. 한국선급은 향후에도 IALA를 비롯하여 적극적으로 국제활동에 참여하여 해상 사이버보안 지침의 표준화를 위해 노력 할 예정이다.

한국선급 활동 #2

TRIPARTITE 2019, 해사 사이버보안 동향 모니터링

한국선급은 최신 해사 사이버보안 동향 모니터링을 위하여 10월 17일~18일 일본 도쿄에서 개최된 세계선주조선선급회의인 TRIPARTITE 2019에 참석하였다. BIMCO(발틱해국제해운협회)와 IACS(국제선급연합회)가 해상 사이버보안 관련 발표를 하였으며 주요내용은 다음과 같다.

◎ BIMCO의 Lars Robert Pedersen은 'Cyber Security Update'란 주제로 각 이해관계자 간 정보 공유의 중요성 및 해사분야의 사이버 리스크 저감을 위한 각 이해관계자의 역할을 강조하였다. 즉 선주는 사이버 리스크를 잘 관리하여야 하고 조선소는 사이버 복원력을 가진 선박을 건조하여야 하며, 기자재업체는 기자재 소프트웨어 개발 시 사이버 리스크를 고려하여 설계 할 것을 당부하였다.

◎ IACS Cyber Systems Panel 의장인 George Reilly 는 'An update on consolidation of cyber recommendations and other planned activities' 란 주제로 IACS의 사이버보안 통합권고서 개발에 대해 소개하였다. 이 통합 권고서는 2018년 배포된 12개의 권고서를 기반으로 이해관계자들의 수요와 기대를 고려하여 개정·통합 되었으며, IMO 가이드라인과 NIST 사이버보안 프레임워크의 5가지 사이버보안 기능 요소(식별, 방어, 탐지, 대응 및 복구)를 IACS 12개 권고서와 매핑하여 신조선 건조를 위한 기능적 요건을 제시하고 있다.

[기획시리즈]③

LTE 구조와 5G의 분산형 네트워크의 비교

본 기획시리즈는 4차산업혁명과 관련한 핵심 통신인프라인 5G가 해양산업에 미칠 긍정적 파급효과와 이에 따른 사이버 위협에 대해 다뤄보고자 한다. 따라서 본 뉴스레터 2019년 9월호에서는 ***'5G 네트워크 구조와 네트워크 슬라이싱 기술***에 대해 소개한다.

기획시리즈 순서

① 5G란 무엇인가?

② 5G의 네트워크 구조와 네트워크 슬라이싱(Network Slicing) 기술, 그리고 해양산업 변화

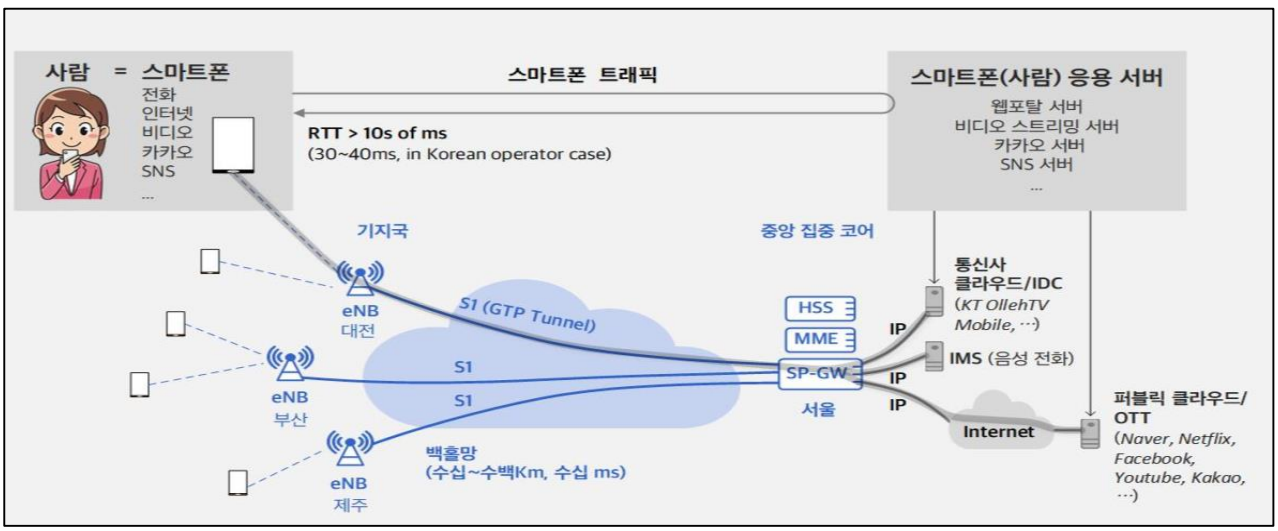
③ LTE의 중앙집중형 네트워크와 5G의 분산형 네트워크의 비교

④ 5G 표준에서 무선백홀 기술과 5G 위성의 역할

⑤ 선박과 항만에 효과적으로 활용하기 위한 5G 표준의 Private Network 참조모델

4G LTE 네트워크 구조

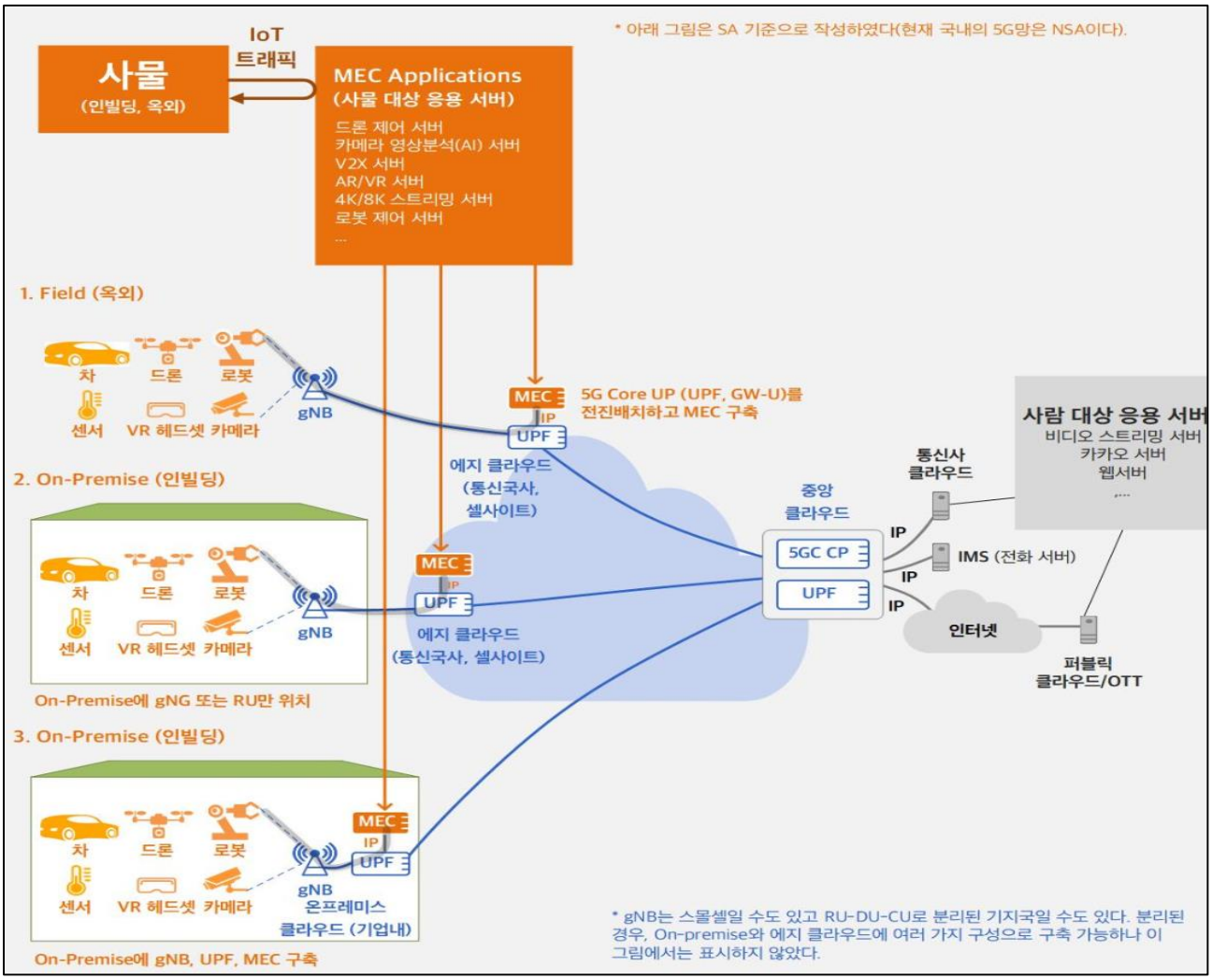
우리가 사용하고 있는 LTE 스마트폰의 네트워크는 무선통신뿐만 아니라 유선통신 네트워크를 포함하고 있다. 4G LTE 유무선 네트워크는 크게 기지국 장비(eNodeB)와 핵심망(Core Network)로 2단계 구조이다. 핵심망은 핸드오버, IP할당, 과금, 정책, 단말기 인증 등의 역할을 하며, LTE Core(SP-GW)는 전국에 몇 개의 사이트에 집중되어 있는 구조이다. 모든 모바일 트래픽이 중앙의 LTE Core(SP-GW)로 전달되며, 이후 IP 라우팅되어 IP 서비스(전화(IMS), 인터넷, OTT 등)를 받을 수 있다. 스마트폰 응용 서비스들이 지연에 매우 민감하지 않고 용량도 많아야 수십 Mbps 정도를 필요로 하므로 4G LTE 네트워크 구조는 스마트폰을 중심으로 특화되어 있다.



출처 : https://www.netmanias.com/ko/post/oneshot/14273/5g-iot-mec/mec-concept-and-deployment-architecture-in-4g-and-5g-network

5G 분산형 네트워크 구조

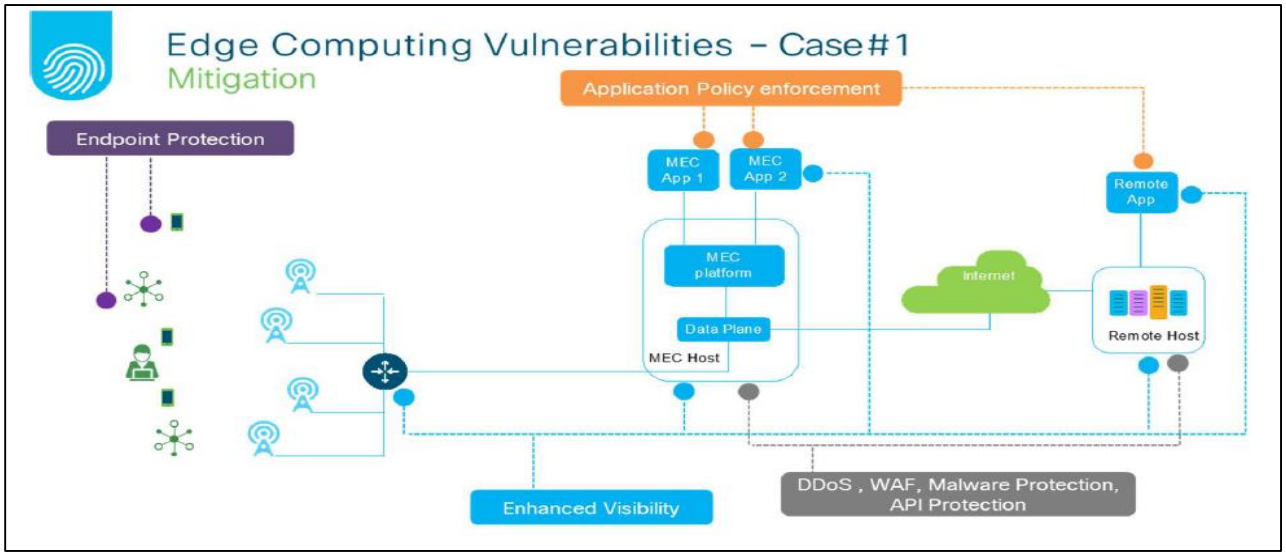
최근 수많은 사물인터넷(IoT; Internet of Things) 기기들이 출현하면서, 기기 간 통신의 신뢰성, 무결성이 중요한 시대가 다가 오고 있다. 예를 들어 자율주행차, 드론 및 로봇제어 등을 위해서는 단말기와 응용서버간의 지연시간과 트래픽 분산문제가 해결되어야 통신의 신뢰성과 무결성을 확보할 수 있다. 하지만 LTE 네트워크는 모든 트래픽들이 LTE Core(SP-GW)로 집중되었다가 IP 라우팅 되는 구조이므로 긴 지연시간이 발생하고, 백홀망 트래픽의 부하를 초래할 수 있다. 이러한 문제를 해결하기 위해 등장한 것이 5G 분산형 네트워크 구조이다. 사물 대상 응용서버(MEC; Mobile Edge Computing)를 단말 가까이 전진 배치하여 초저지연 응답을 제공하고, 백홀망의 트래픽을 절감할 수 있는 효과가 있다. 이러한 5G의 분산형 네트워크 구조를 선박 내부 네트워크에 적용한다면 선내의 수많은 센서와 기기제어, 선내 CCTV 영상분석을 통한 선내 모니터링 서비스를 효과적으로 구현하고, 화물(컨테이너 등)에 사물인터넷(IoT) 기기를 부착함으로써, 해운물류 서비스의 혁신을 초래할 수 있을 것으로 본다.



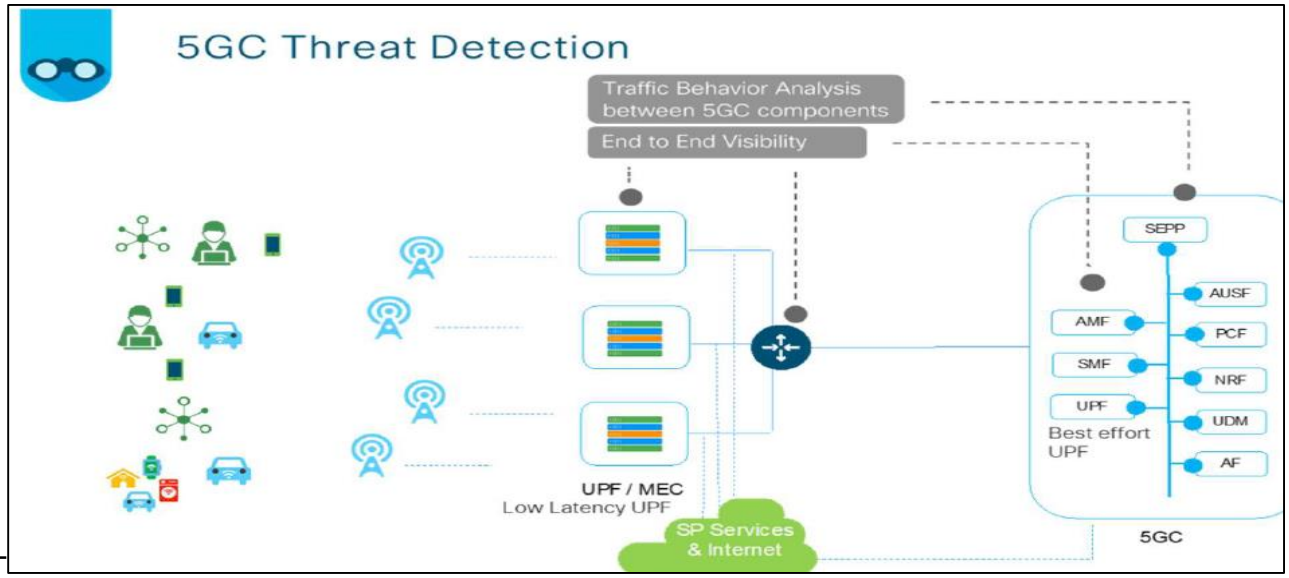
출처 : https://www.netmanias.com/ko/post/oneshot/14273/5g-iot-mec/mec-concept-and-deployment-architecture-in-4g-and-5g-network

5G의 사이버보안 위험요소 - 5G 분산형 네트워크 구조의 보안 취약점

5G 분산형 네트워크 구현하기 위해서는 다양한 네트워크 슬라이스가 서버, 메모리, 네트워크 및 스토리지와 같은 물리적 인프라를 공유하게 된다. 이러한 경우 각 슬라이스에 대한 자원 예약 및 격리는 본질적으로 가변적일 수 있으며, 공통 자원 풀 세트를 공유할 수 있다. 이러한 경우, 하나 이상의 슬라이스에 대한 DoS/DDoS 유형 공격은 간접적으로 다른 슬라이스에 영향을 줄 수 있다. 따라서 물리적 인프라는 다양한 슬라이스에서 공통 리소스를 공유할 때, 슬라이스 간에 적절한 리소스 격리를 제공해야 한다.



이러한 5G 분산형 네트워크의 보호를 위해서는 적절한 가시성, 세그멘테이션, DNS 레벨 보안(예 : 알려진 취약점, 악성 도메인) 및 비정상 네트워크 흐름탐지가 필수적이다.
적절한 가시성과 행동분석을 통해 운영자가 5G 네트워크 코어에 영향을 미치는 위협을 탐지 할 수 있다.



출처 : The Evolution of Security in 5G, 5G America white paper, July 2019

사이버 위협의 이해(OWASP Top 10)

사이버 위협 이해하기

사이버 위협이란, 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 대해 사이버 시스템을 통한 무단 액세스, 파괴, 공개, 정보 수정 또는 서비스 거부와 같은 잠재적으로 악영향을 미칠 수 있는 상황이나 사건을 의미한다. (출처 : NIST SP : 800-128)

사이버위협은 ICT 기술이 발전함에 따라 자산에 미치는 영향이 변화하므로 자산의 취약점을 파악하기 위해 주기적으로 목록화 할 필요가 있다.

한국선급 해상 사이버보안 시스템 인증 검사항목(CS1)

204.1 위험관리 : 내부 정보기술 및 운영기술 환경에 의한 영향을 미치는 외부 환경 요인을 위협으로 식별하고 목록화하여야 한다.

OWASP Top 10

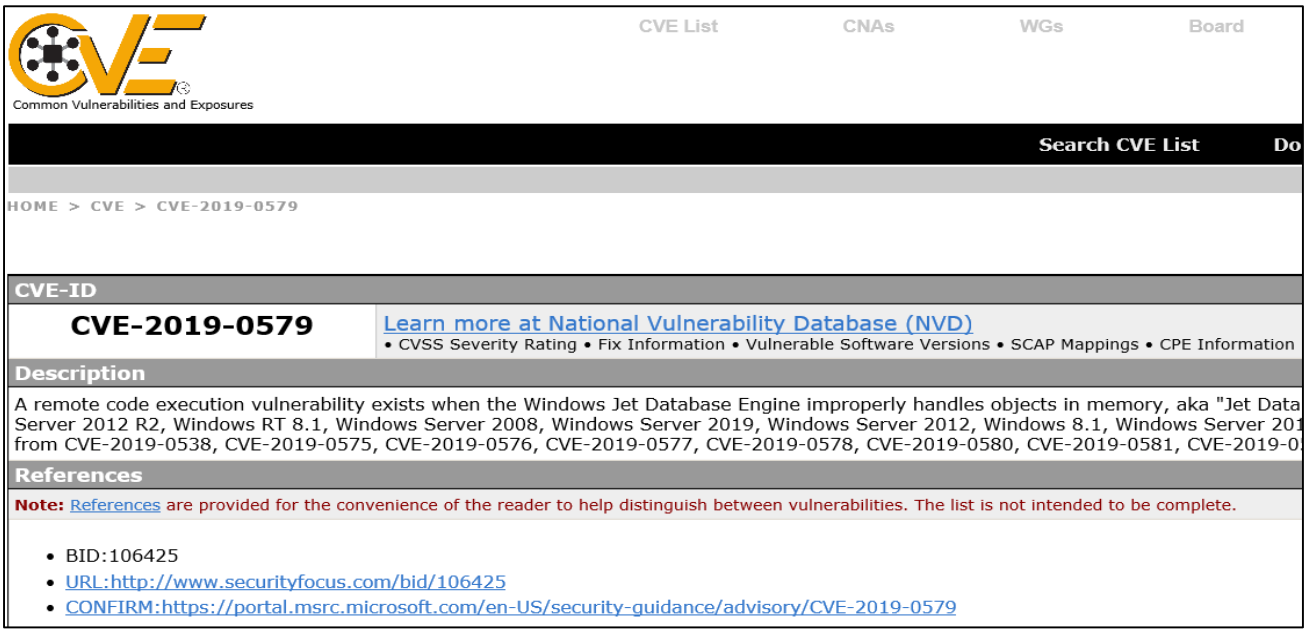
OWASP(Open Web Application Security Project)는 오픈소스 웹 어플리케이션 보안 프로젝트이다. 주로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며 웹 어플리케이션 취약점 중에서 빈도가 높고, 보안상 영향을 크게 줄 수 있는 10대 항목(OWASP Top 10)을 2004년, 2007년, 2010년, 2013년, 2017년 기준으로 발표하였다. 1월 뉴스레터에 이어 **'A9 : 2017 – 알려진 취약점이 있는 구성요소 사용'**를 분석하고자 한다.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – 인젝션	→	A1:2017 – 인젝션
A2 – 취약한 인증과 세션 관리	→	A2:2017 – 취약한 인증
A3 – 크로스 사이트 스크립팅 (XSS)	↘	A3:2017 – 민감한 데이터 노출
A4 – 안전하지 않은 직접 객체 참조 [A7 항목과 병합됨]	∪	A4:2017 – XML 외부 개체 (XXE) [신규]
A5 – 잘못된 보안 구성	↘	A5:2017 – 취약한 접근 통제 [합침]
A6 – 민감한 데이터 노출	↗	A6:2017 – 잘못된 보안 구성
A7 – 기능 수준의 접근 통제 누락 [A4 항목과 병합됨]	∪	A7:2017 – 크로스 사이트 스크립팅 (XSS)
A8 – 크로스 사이트 요청 변조 (CSRF)	☒	A8:2017 – 안전하지 않은 역직렬화 [신규, 커뮤니티]
A9 – 알려진 취약점이 있는 구성요소 사용	→	A9:2017 – 알려진 취약점이 있는 구성요소 사용
A10 – 검증되지 않은 리다이렉트 및 포워드	☒	A10:2017 – 불충분한 로깅 및 모니터링 [신규, 커뮤니티]

출처 : OWASP Top 10 Project

OWASP 10대 위협 'A9 : 2017 - 알려진 취약점이 있는 구성요소 사용'

제로 데이 (Zero-day) 취약점은 공개되지 않은 소프트웨어, 하드웨어 또는 펌웨어의 결함을 의미하며 보안패치가 나오지 않은 상태이다. 원데이(1-day) 취약점은 공개된 취약점이나 보안패치를 적용하지 않은 상태이다. 해커는 최신 취약점이기 때문에 구성요소가 보안 패치를 적용하기까지 시간이 걸리는 점을 이용한다. 민약 구성요소가 마이크로소프트 제품 원격코드실행(RCE) 취약점인 "CVE-2019-0579"를 패치하지 않았다면 별도의 인증없이 관리자 권한 명령어 실행이 원격으로 가능하게 된다. 아래의 MITRE에서 제공하는 데이터베이스를 활용하면 원데이 취약점을 예방하기 위한 대책을 수립하는데 도움이 될 것으로 예상된다.



CVE
Common Vulnerabilities and Exposures

CVE List CNAs WGs Board

Search CVE List Do

HOME > CVE > CVE-2019-0579

CVE-ID

CVE-2019-0579

Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Data Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 201 from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0580, CVE-2019-0581, CVE-2019-0

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:106425
- URL:http://www.securityfocus.com/bid/106425
- CONFIRM:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0579

출처 : https://cve.mitre.org/

취약점 확인 방법

- 클라이언트와 서버 측면의 양쪽에서 사용하는 모든 구성 요소의 버전을 알지 못한다면, 취약할 가능성이 있습니다. 여기에는 직접 사용하는 구성 요소와 중첩된 종속성이 포함됩니다.
- 소프트웨어가 취약하거나, 지원되지 않거나, 오래된 버전인 경우, 취약할 가능성이 있습니다. 여기에는 운영체제, 웹/애플리케이션 서버, 데이터베이스 관리 시스템(DBMS), 애플리케이션, API와 모든 구성요소, 런타임 환경과 라이브러리 등이 포함됩니다.
- 정기적으로 취약점을 스캔하지 않거나, 사용 중인 컴포넌트와 관련된 보안 취약점 공지 서비스에 등록하지 않은 경우, 취약할 가능성이 있습니다.
- 위험 기반으로 적절한 시기에 플랫폼, 프레임워크와 종속성을 수정하거나 업그레이드하지 않은 경우, 취약할 가능성이 있습니다. 이는 패치 적용이 변경 통제 하에서 매월 또는 분기별 작업하는 환경에서 일반적으로 발생합니다. 이로 인해 조직은 며칠 또는 몇 달 동안 수정된 취약점에 불필요하게 노출될 수 있습니다.
- 소프트웨어 개발자가 업데이트된, 업그레이드된 혹은 패치된 라이브러리의 호환성을 테스트하지 않는다면 취약할 가능성이 있습니다.
- 구성요소의 구성 정보를 보호하지 않는다면, 취약할 가능성이 있습니다. (**A6:2017-잘못된 보안 구성**을 보십시오).

보안 대책

패치 관리 프로세스가 있어야만 합니다:

- 사용하지 않는 종속성, 불필요한 기능, 구성 요소, 파일과 문서 등을 제거하십시오.
- versions, DependencyCheck, retire.js 와 같은 도구를 사용하여 클라이언트 및 서버 측의 구성 요소(예: 프레임워크, 라이브러리) 와 해당 종속성의 버전을 지속적으로 관리합니다. CVE 와 NVD로부터 구성요소 내 취약점을 지속적으로 모니터링합니다. 소프트웨어 구성 분석 도구를 사용하여 프로세스를 자동화 하십시오. 사용하는 구성요소와 관련된 보안 취약점에 대한 전자메일 알림을 구독하십시오.
- 안전한 링크를 통해 공식적인 출처로부터 구성 요소를 획득하십시오. 조작되거나, 악의적인 구성 요소가 포함될 가능성을 줄이기 위해 서명된 패키지를 사용하십시오.
- 유지 관리되지 않거나, 이전 버전의 보안 패치를 만들지 않는 라이브러리 및 구성 요소를 모니터링합니다. 패치가 불가능한 경우, 발견된 문제를 모니터링, 탐지 혹은 보호하기 위해 가상 패치를 배포하는 것을 고려하십시오.

모든 조직은 애플리케이션 혹은 포트폴리오의 수명 주기 동안 업데이트 또는 구성 변경을 모니터링, 검토 및 적용하기 위한 지속적인 계획이 있는지를 확실히 해야만 합니다.

출처 : OWASP Top 10 - 2017

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

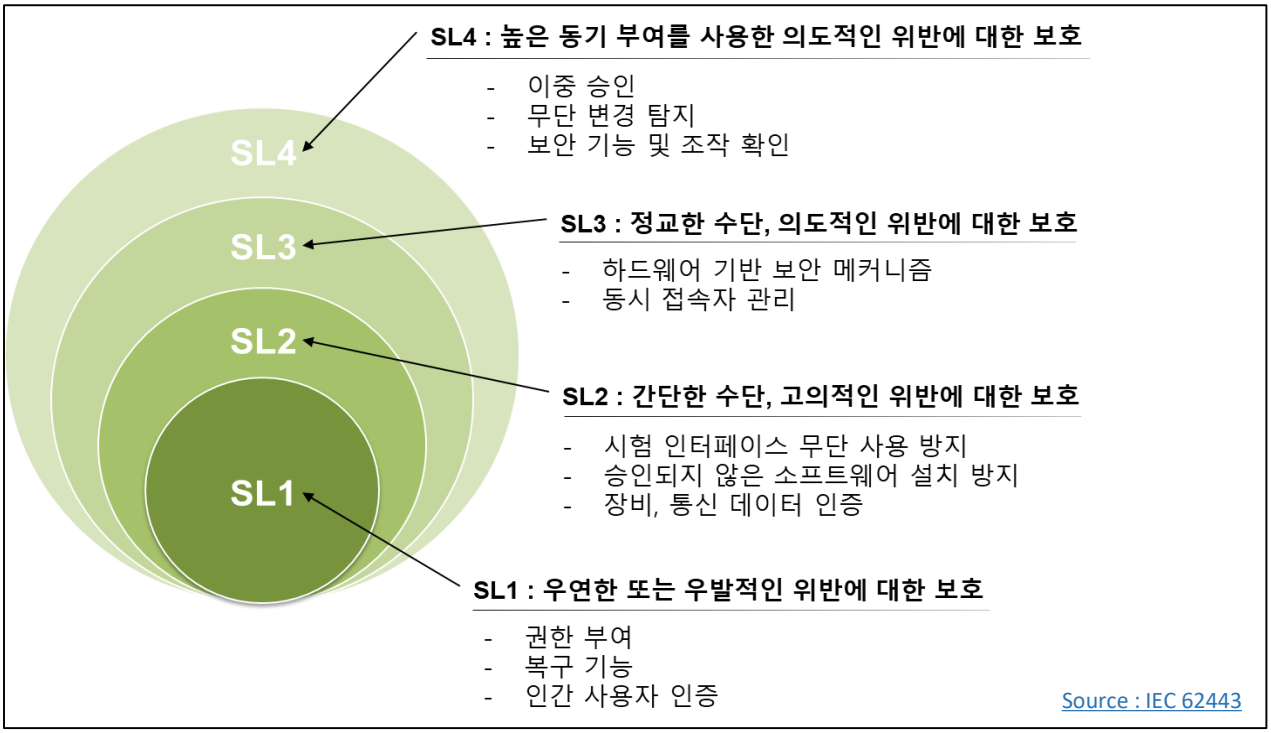
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<KR 사이버보안 형식승인 지침의 구성>

제1절 : 일반사항	제5절 : 데이터 기밀성	제9절 : SW 애플리케이션 요건
제2절 : 식별 및 인증	제6절 : 제한된 데이터 흐름	제10절 : 임베디드 장비 요건
제3절 : 사용 제어	제7절 : 사고에 대한 적시 대응	제11절 : 호스트 장비 요건
제4절 : 시스템 무결성	제8절 : 리소스 가용성	제12절 : 네트워크 장비 요건

Source : http://www.krs.co.kr/KRRules/KRRules2019/data/data_other/ENGLISH/gc31e000.pdf

보안등급(SL, Security Level)의 이해



Source : IEC 62443

한국선급 해상 사이버보안 형식인증 검사항목

소프트웨어 및 정보 무결성 (403)

1. 구성품은 구성에 대한 무결성 검사를 수행할 수 있는 기능을 제공하여야 한다.(SL1)
2. 구성품은 진본성 점검을 수행할 수 있는 기능을 제공하여야 한다.(SL2)
3. 무단 변경을 시도하는 것을 발견하면 통지하는 기능을 제공하여야 한다.(SL3,4)

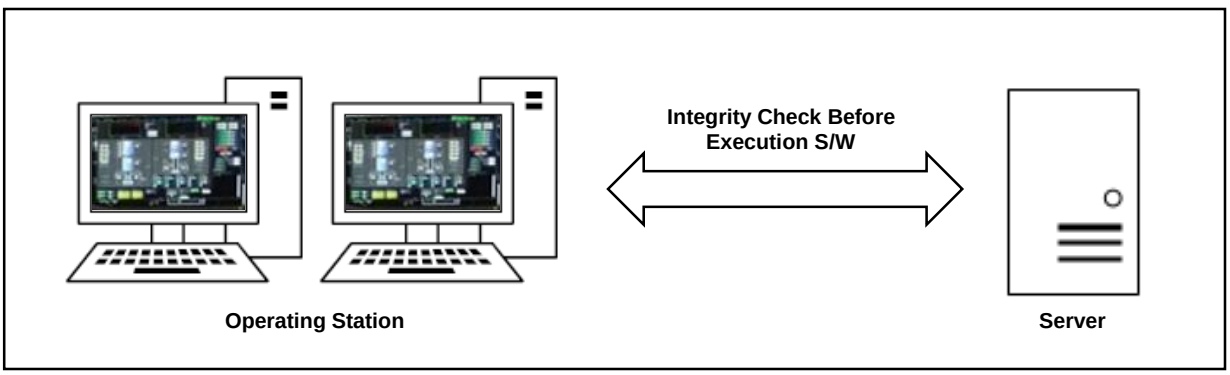
한국선급이 사이버보안 형식승인에서 무결성을 확인하는 이유는 무엇일까?

소프트웨어와 정보 무결성은 사이버 시스템의 정확성과 완전성을 보호하는 성질을 의미한다. 선박에는 수 많은 시스템들이 설치되어 있기 때문에 각 시스템에서 발생된 정보들이 정확한 정보가 아닐 가능성이 존재 할 수 있는 것이다. 예를 들어 선박의 알람모니터링 시스템(AMS)이 메인엔진에 설치된 임의의 센서로부터 입출력 장치의 무단 변경으로 인해 알람을 받았을 때, 이 알람이 중요한 정보임에도 불구하고, 기관사에게 정확한 정보가 전달되지 않는다면, 심각한 안전 사고로 이어질 수 있다. 한국선급의 사이버보안 형식승인에서는 이러한 문제를 방지하기 위한 기술적인 기능을 확인하는 것이다.

'SL 1'에서는 시스템 구성에 대한 무결성을 확인할 수 있는 기능을 요구한다. 예를 들어, 시스템 구성도(System Configuration) 상에 장비들의 배치, 연결 정보등을 확인하고, 이에 대한 변경이 발생할 경우 사용자가 확인 할 수 있도록 하는 방법이 있을 수 있다. 소프트웨어의 구성요소들을 점검하여 위조/변조가 없음을 확인 후 프로그램을 실행하는 기능이 될 수 있다.

'SL 2'에서는 진본성 (Authenticity) 점검 기능을 요구한다. 진본성이란 인증과 무결성 검증을 통해 자산의 소유권이 주장한대로 임을 확인하는 성질을 의미한다. 예를 들어, 정품 소프트웨어 인증 혹은 정품 인증서(Certification of Authenticity)가 될 수 있다. 하드웨어에 대한 진본성 점검 기능으로는 구성품의 고유한 정보를(시리얼번호 등) 확인하고, 이에 대한 인증을 수행하여 임의의 구성품 변경이 불가하도록 요구하고 있다.

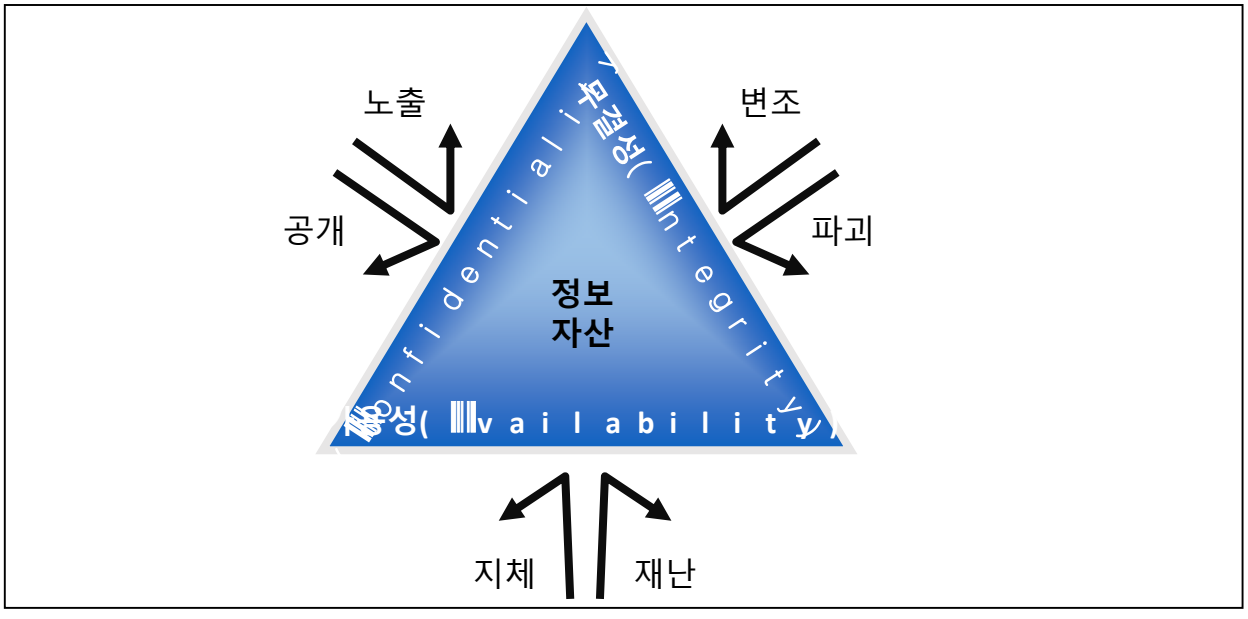
'SL 3,4'에서는 무단 변경이 불가할 뿐 아니라 이에 대한 알람 기능을 요구하고 있다.



용어 설명

사이버보안의 3요소

사이버보안이란 사이버 자산을 공개/노출, 변조/파괴, 지체/재난 등의 위협으로부터 보호하여 정보의 기밀성, 무결성, 가용성을 확보하는 것을 의미한다. 사이버보안의 3요소는 다음과 같다.



- 기밀성(Confidentiality) : 인가되지 않은 방식으로 정보를 획득 할 수 없도록 하는 것
- 무결설(Integrity) : 데이터나 리소스를 인증되지 않은 변경으로부터 보호하는 것
- 가용성(Availability) : 인가를 받은 사용자가 정보나 서비스를 요구할 경우 정보시스템에 대한 사용가능의 요구사항