KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 018

October 2019

KR Cyber Security Activities

- IALA ENAV24 Committee for Maritime Cyber Security Standardization
- KR attended Tripartite 2019 to monitor Maritime Cyber Security Trends
-

[Series news] ③ LTE and 5G Network Architecture

Understanding Cyber Threats(OWASP Top 10)

Guidelines for Type Approval of Maritime Cyber Security

Explanation of Term

KR attended IALA ENAV24 for Maritime Cyber security Standardization

Korean Register of Shipping (KR) attended the 24th IALA (International Association of Lighthouse Authorities) ENAV committee on Maritime Cyber Security Standardization, held in Paris, France, from October 7 to 11. IALA is an international organization that is leading the standardization of e-Navigation and digital maritime communication. As the possibility of exposure to cyber threats increases due to the emerging digital technology in international maritime domain such as IMO, BIMCO, and CIRM, IALA also has been regarded as an important issue in discussing standardization for cyber security application to AtoN (Aid to Navigation) and VTS (Vessel Traffic Service). At the IALA ENAV 24 meeting, IALA announced the plans to develop the cyber security Guidelines/Recommendation. KR participated in IALA's cyber security standardization discussion and announced the formal approval guidelines and actual application cases developed by KR, and was asked to continue cooperation by many government representatives and industry member companies participating in the IALA ENAV Committee. KR developed type approval guidelines are based on international standards (IEC 62443 4-2 and IEC 61162-460, etc.), and have been implemented a service such as the HYUNDAI-ISCS, a smart integrated communication equipment for ships developed by Hyundai Heavy Industries. KR will actively participate in international activities including IALA in the future and strive to standardize maritime cyber security guidelines.

KR Cyber security Activities #2

KR attended Tripartite 2019 to monitor maritime cybersecurity trends

Korean Register of Shipping(KR) attended the Tripartite Meeting 2019 at the World Shipbuilding Conference, held in Tokyo, Japan, 17-18 October, to monitor the latest maritime cybersecurity trends. BIMCO (Baltic and International Maritime Council) and IACS (International Association of Classification Societies) gave a presentation on maritime cyber security.

Lars Robert Pedersen from BIMCO emphasized the importance of information sharing amongst stakeholders and the important role each stakeholder plays in reducing cyber risk across the maritime sector. In other words, ship owners should manage cyber risks well, shipyards should build ships with cyber resilience, and equipment manufacturers should design the cyber software with due consideration of the cyber risks.

George Reilly, Chairman of IACS Cyber Systems Panel, introduced IACS's cyber security advisory entitled 'An update on consolidation of cyber recommendations and other planned activities'. This integrated recommendation was revised and integrated based on 12 recommendations distributed in 2018, considering the needs and expectations of stakeholders. The five cyber security functional elements (identification, defense, detection, response and recovery) of the IMO guidelines and the NIST cyber security framework are mapped with 12 recommendations of IACS to suggest functional requirements for the construction of new shipbuilding.

TRIPARTITE 2019
THE SHIPBUILDERS' ASSOCIATION OF JAPAN
ClassNK
JSA
INTERCARGO
INTERCARGO
International Association of Dry Cargo Shipowners
TRIPARTITE 2019 TOKYO
18 October
Session 6 Pollution Prevention

[Series news] ③

LTE and 5G Distributed Network Architecture

This series will deal with a core infrastructure related to the 4th industrial revolution, the positive ripple effect of 5G on the marine industry, and the cyber threat accordingly. Therefore, this newsletter, Sep. 2019, introduces '5G network structure and network slicing technology.

series news

① What is 5G?

② 5G Network architecture - Network Slicing, and Affects on the maritime Industry

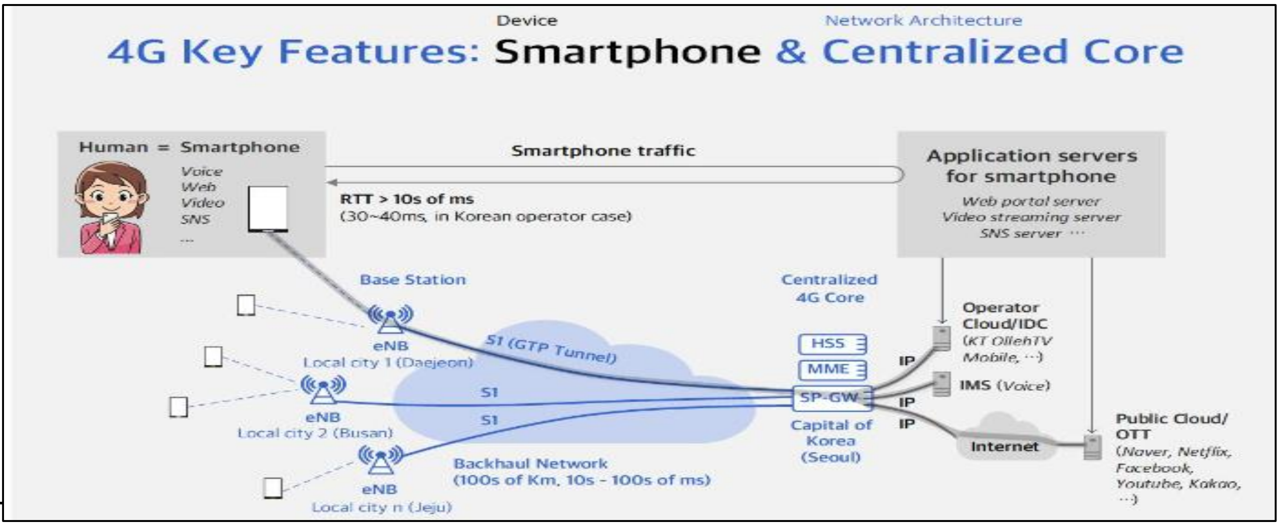
③ **Comparison between LTE centralized network and 5G distributed network**

④ Role of wireless backhaul technology and 5G satellites in 5G standards

⑤ The private network reference model in 5G standard for effective use in ships and ports

4G LTE Network Architecture

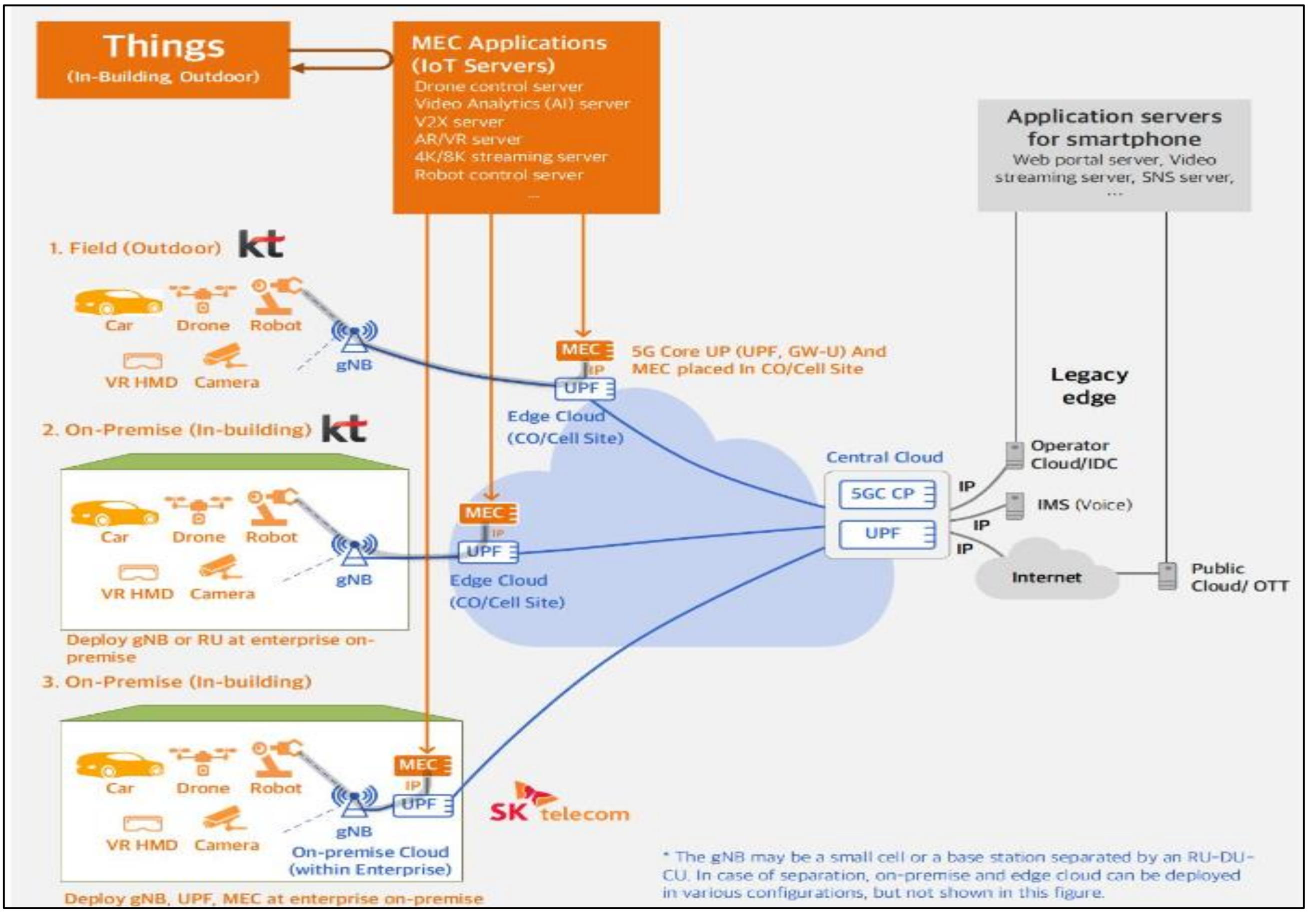
Today's LTE smartphones includes wired networks as well as wireless communication. LTE wired and wireless networks are largely two-step structures with base station equipment (e Node B) and a core network. The core network plays the role of handover, IP allocation, charging, policy, and terminal authentication, while the LTE Core (SP-GW) is a structure based on several sites nationwide. All mobile traffic is delivered to the central LTE Core (SP-GW), and then via IP routing, it can receive IP services (i.e., voice (IMS), the Internet, OTT, etc.). Since smartphone application services are not very sensitive to delays and require dozens of Mbps because of their high capacity, the 4GLTE network structure is mainly specialized on smartphones.



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

5G distributed network architecture

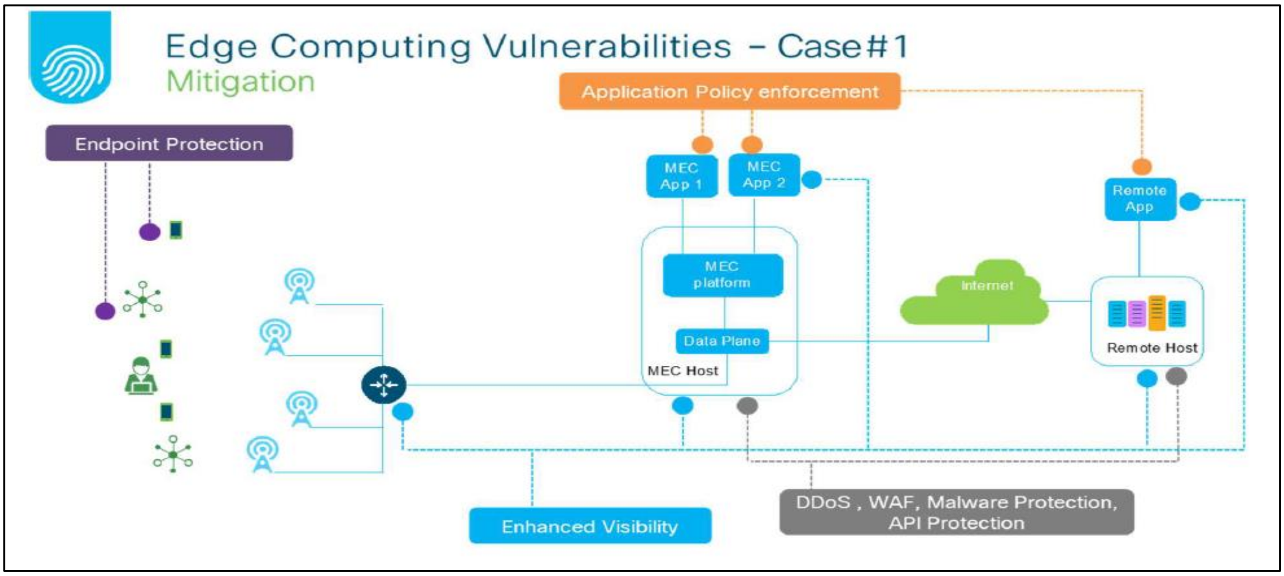
With the emergence of many Internet of Things (IoT) devices, a new era of reliability and integrity of communication between devices is approaching. For example, in order to control autonomous vehicles, drones, and robots, the delay time and traffic distribution between the terminal and the application server must be resolved in order to ensure the reliability and integrity of communication. However, an LTE network is a structure in which all traffic is concentrated on LTE Core (SP-GW) and then IP routing, so there is a long delay time and backhaul traffic load can result. To solve this problem, a 5G distribution network structure is appearing. The present invention provides an ultra-low delay response by forwardly arranging a mobile edge computing (MEC) to be an object near a terminal and reduces the traffic of a backhaul network. If the distributed network structure of 5G is applied to an internal network of a ship, a monitoring service on a ship is effectively implemented through numerous sensors, device control, and on-board CCTV image analysis, and an IoT device can be installed on a cargo (container, etc.) attaching this can significantly enhance the shipping logistics service, offering opportunities for innovation.



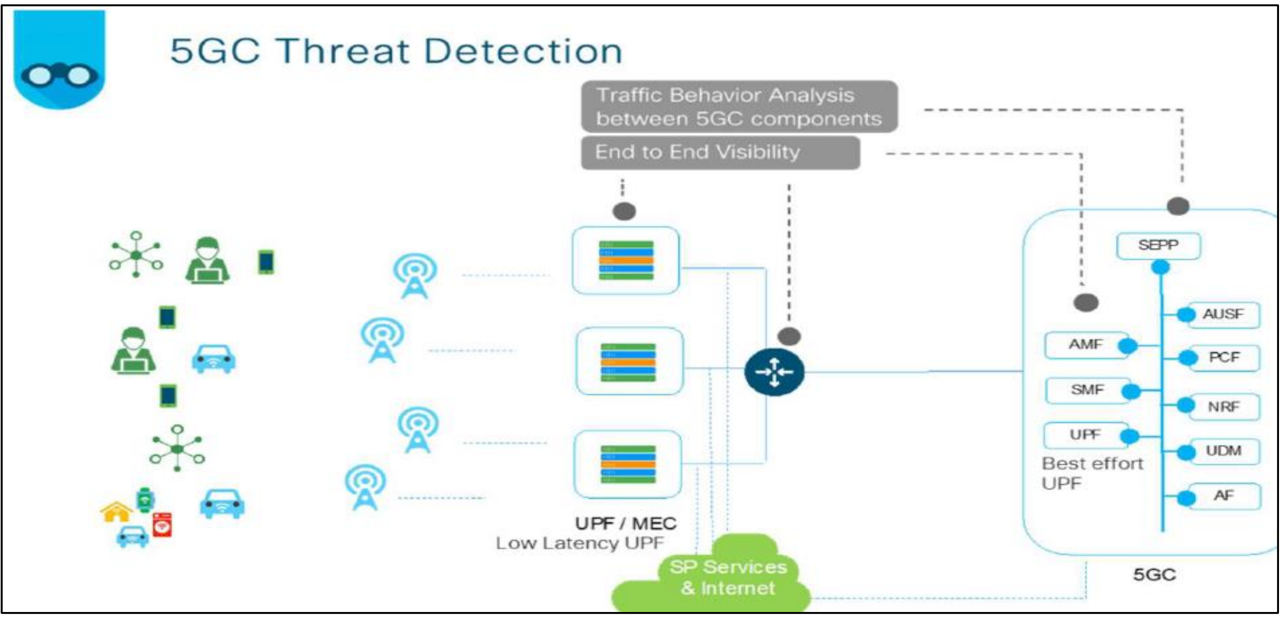
Source : https://www.netmanias.com/ko/post/oneshot/14273/5g-iot-mec/mec-concept-and-deployment-architecture-in-4g-and-5g-network

5G cyber security risk factors - Vulnerabilities of 5G distributed network

Across a 5G distributed network, various network slices may share physical infrastructure such as servers, memory, networks and storage. In such cases, resource reservations and isolation for each slice may be variable, and they may share a common resource pool set. As a result, DoS/DDoS type attacks on one or more slices may indirectly affect other slices. Therefore, physical infrastructures should be designed to provide appropriate resource isolation between slices when sharing common resources.



Proper visibility, segmentation, DNS level security (for example, known bad talkers, bad domains) and detection of abnormal flows is essential. The appropriate visibility and behavior analysis can then detect any malicious operator or actions affecting the 5G network core. proper visibility and behavior analysis allows the operator to detect threats impacting the 5G network core.



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

Understanding Cyber Threats(OWASP Top 10)

Understanding cyber threats

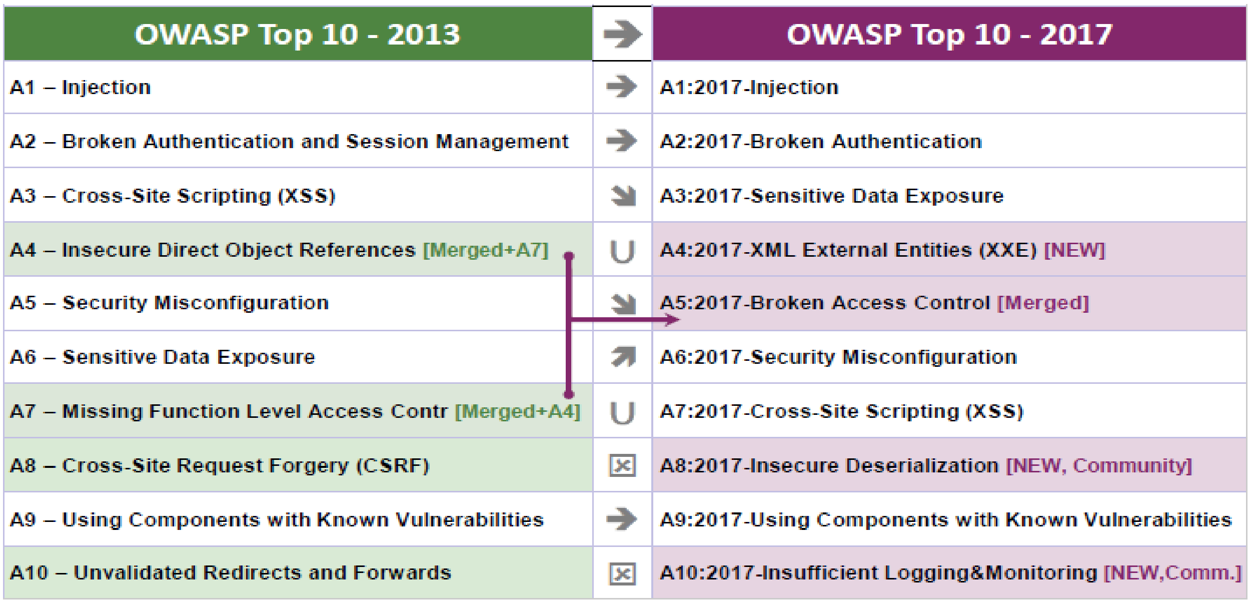
A cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, or the nation state through unauthorized access to an information system, causing destruction, disclosure, modification of information, and/or denial of service (source: NIST SP: 800-128). Cyber threats need to be categorized periodically to identify the vulnerabilities of assets, and the potential impact on that asset.

KR Guidance for Maritime Cyber Security System requirement(CS1)

204.1 Risk Management : External environmental factors affecting the environments of internal information technology and operational technology should be identified and cataloged as threats.

OWASP Top 10

The Open Web Application Security Project (OWASP) is an open source web application security project, researching web exposure, malicious files and scripts, and security vulnerabilities. The OWASP Top 10, which is frequently referred to, highlights the top web application vulnerabilities, it was published in 2004, 2007 , 2010, 2013 and 2017. In this newsletter we will analyze the **'A8 : 2017 – Using Components with Known Vulnerabilities'**

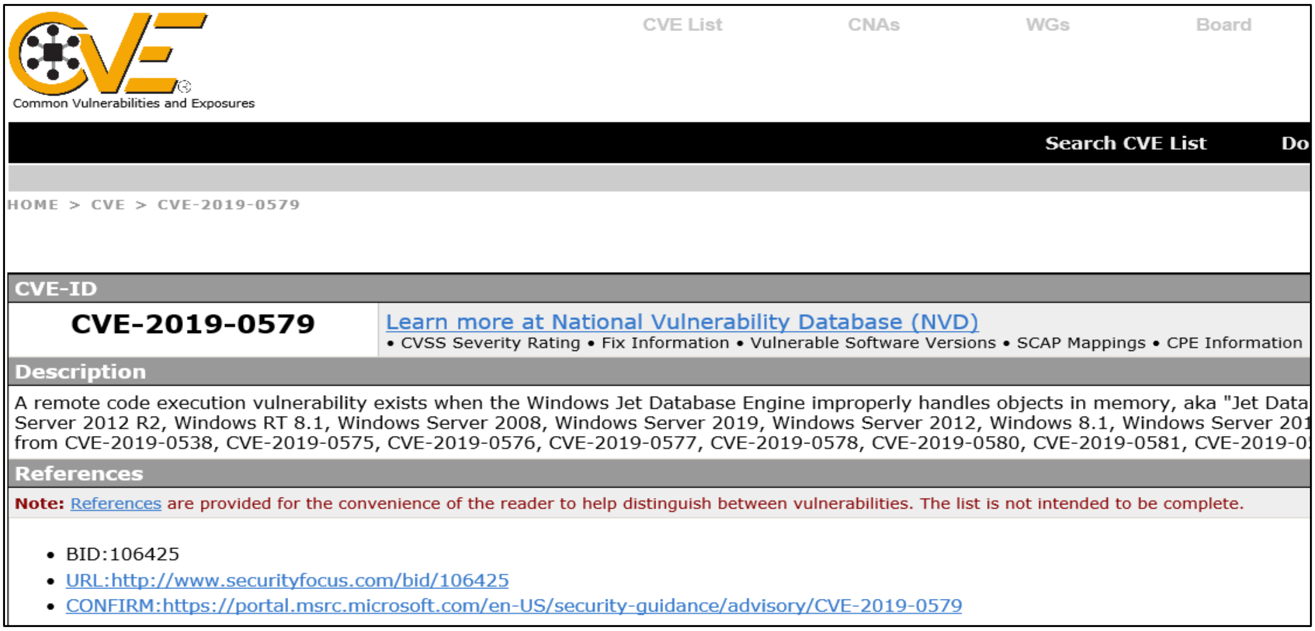


OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Source : OWASP Top 10 Project

OWASP Top 10 'A8 : 2017 -Using Components with Known Vulnerabilities'

Zero-day vulnerabilities are defects in software, hardware, or firmware that are not disclosed, and no security patch has been released. One-day vulnerability does not apply public vulnerability or security patch; Hackers uses this vulnerability components because they are the latest vulnerability and take a long time to apply security patches. If the weak components do not patch using the Microsoft product remote code execution (RCE) vulnerability, "CVE-2019-0579", the executive authority command execution will be possible to apply remotely without any additional authentication. The database provided by MITRE below is expected to help to establish countermeasures to prevent one-day vulnerability.



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

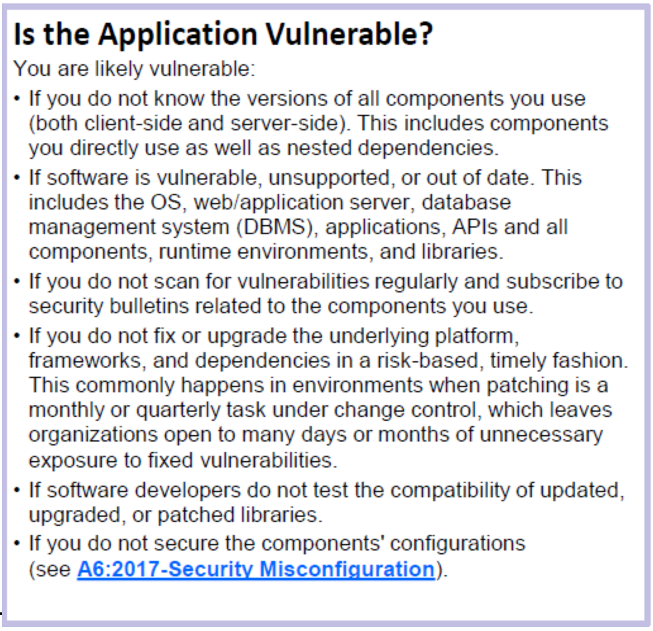
Description

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.

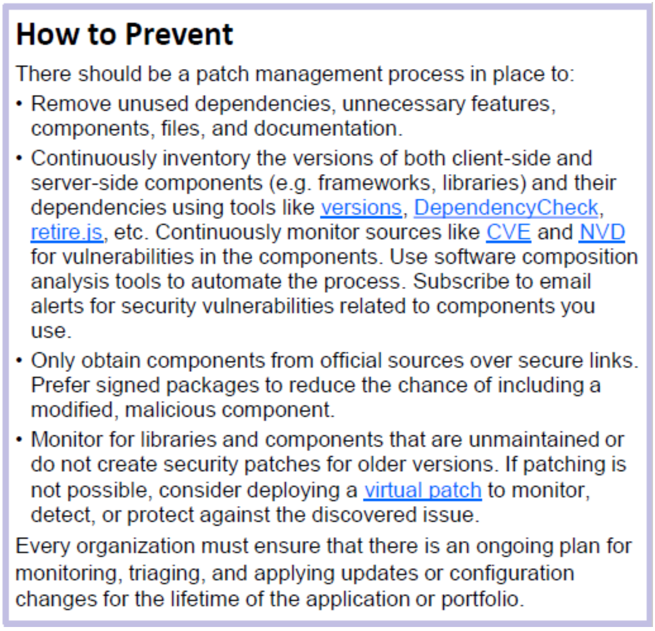
- BID:106425
- URL:http://www.securityfocus.com/bid/106425
- CONFIRM:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0579



Is the Application Vulnerable?

You are likely vulnerable:

- If you do not know the versions of all components you use (both client-side and server-side). This includes components you directly use as well as nested dependencies.
- If software is vulnerable, unsupported, or out of date. This includes the OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries.
- If you do not scan for vulnerabilities regularly and subscribe to security bulletins related to the components you use.
- If you do not fix or upgrade the underlying platform, frameworks, and dependencies in a risk-based, timely fashion. This commonly happens in environments when patching is a monthly or quarterly task under change control, which leaves organizations open to many days or months of unnecessary exposure to fixed vulnerabilities.
- If software developers do not test the compatibility of updated, upgraded, or patched libraries.
- If you do not secure the components' configurations (see **A6:2017-Security Misconfiguration**).



How to Prevent

There should be a patch management process in place to:

- Remove unused dependencies, unnecessary features, components, files, and documentation.
- Continuously inventory the versions of both client-side and server-side components (e.g. frameworks, libraries) and their dependencies using tools like versions, DependencyCheck, retire.js, etc. Continuously monitor sources like CVE and NVD for vulnerabilities in the components. Use software composition analysis tools to automate the process. Subscribe to email alerts for security vulnerabilities related to components you use.
- Only obtain components from official sources over secure links. Prefer signed packages to reduce the chance of including a modified, malicious component.
- Monitor for libraries and components that are unmaintained or do not create security patches for older versions. If patching is not possible, consider deploying a virtual patch to monitor, detect, or protect against the discovered issue.

Every organization must ensure that there is an ongoing plan for monitoring, triaging, and applying updates or configuration changes for the lifetime of the application or portfolio.

Source : OWASP Top 10 - 2017

Guideline for Type Approval of Maritime Cyber Security

Understanding Guideline for Type Approval of Maritime Cyber Security

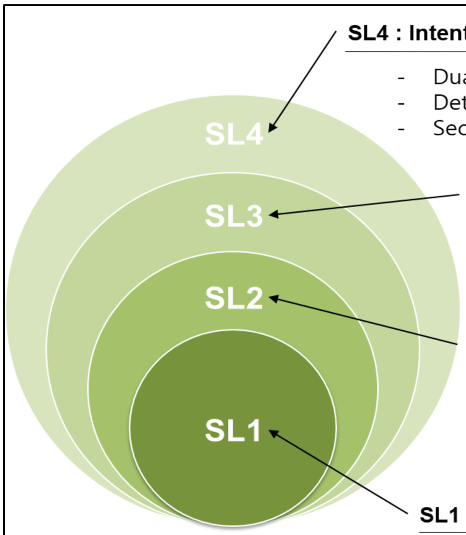
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance before installation on board. The cyber security type approval has been developed based on international standards such as ISA 62443 4-2, IEC 61162-460, and inspect cyber security level and function of cyber systems including remote access equipment, integrated control and monitoring systems on board the ship. The security requirements and their levels are verified on 12 categories and 124 requirements.

< Composition of KR Cyber Security Type Approval Guidelines >

Section 1 General	Section 5 Data Confidentiality	Section 9 Software Application Requirements
Sections 2 Identification and Authentication	Section 6 Restricted Data Flow	Section 10 Embedded Device Requirements
Section 3 Use Control	Section 7 Timely Response to Events	Section 11 Host Device Requirements
Section 4 System Integrity	Section 8 Resource Availability	Section 12 Network Device Requirements

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

Understanding Security Level (SL)



SL4 : Intentional violation, sophisticated means with extended resources

- Dual Approval
- Detect unauthorized alteration
- Security functionality and operation verification

SL3 : Intentional violation, sophisticated means with moderate resources

- Security mechanism based on hardware
- Concurrent session control

SL2 : Intentional violation, simple means with low resources

- Protect against unauthorized use of test interface
- Protect from installation and execution of unauthorized software
- Device, communication data identification and authentication

SL1 : Casual or coincidental violation

- Authorization
- Backup and restore
- Human user authentication

Source : IEC 62443

KR Type Approval of Maritime Cybersecurity Inspection Items

Software and information integrity (403)

1. Components should provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks.(SL1)
2. Components should provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system.(SL2)
3. If the component is performing the integrity check, it should be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.(SL3,4)

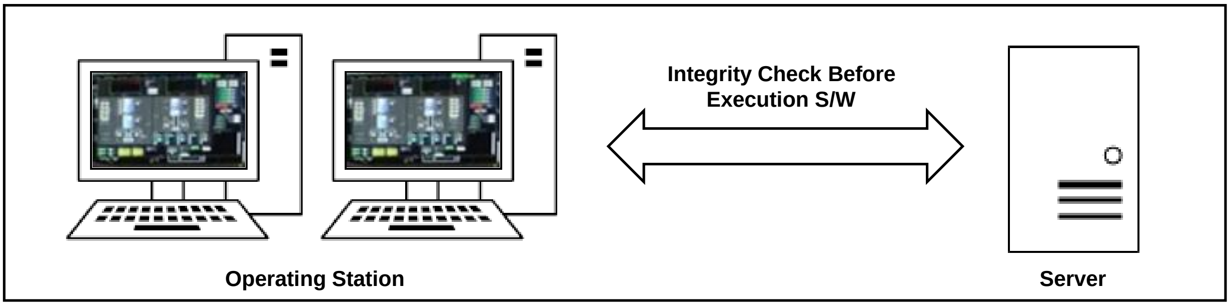
Why does KR check integrity in cyber security type approval?

Software and information integrity means protecting the accuracy and completeness of cyber systems. Since there are many systems installed in the ship, there is a possibility that the information generated in each system is not accurate information. For example, when the ship's alarm monitoring system (AMS) is alarmed by unauthorized change of the input/output device from any sensor installed in the main engine, if the correct information is not delivered to the engineer, it can lead to serious safety accidents. KR's cyber security format approval is to confirm the technical function to prevent this problem.

'**SL1**' requires the function to confirm the integrity of the system configuration. For example, there may be a method to check the arrangement of equipment, connection information, etc. on the system configuration, and to allow the user to check if a change occurs. It can be a function of checking the components of the software to check for forgery/modulation and then running the program.

'**SL2**' requires the authenticity check, which means confirming the accuracy of assets through authentication and integrity verification. For example, it can be a software authentication or a certificate of authenticity. The authenticity check function for hardware is to check the unique information of the components (such as serial number) and perform authentication for it to require that any component change is not possible.

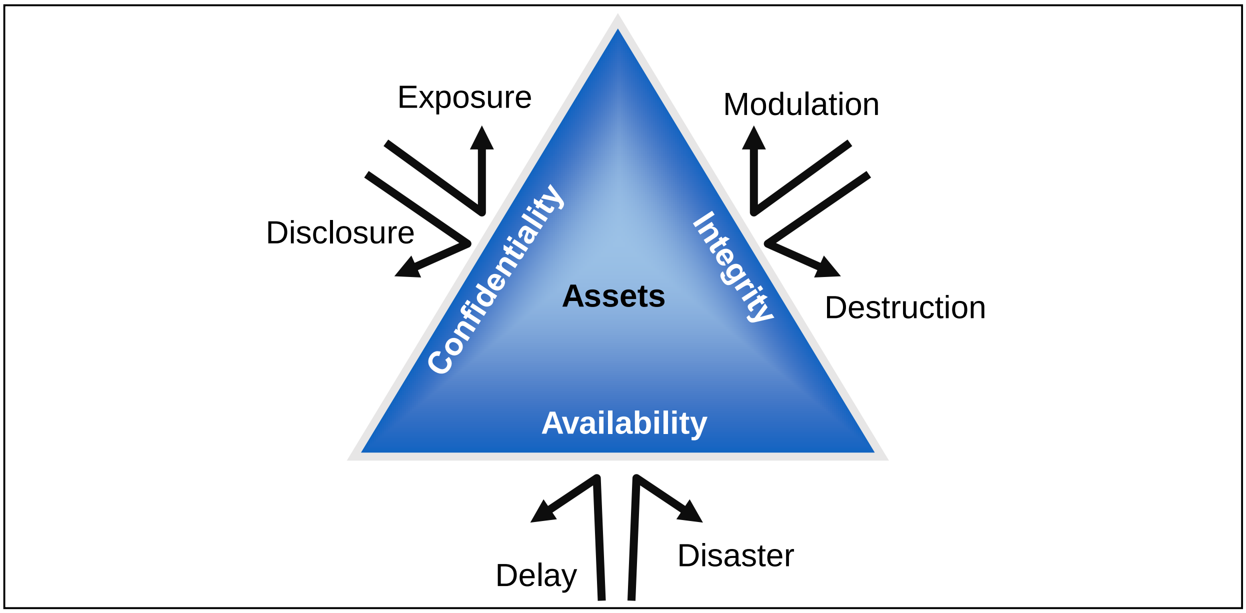
'**SL3,4**' requires that do not permit to change the system as well as alarm function if changed.



Explanation of Term

Three elements of cyber security

Cyber security means securing the confidentiality, integrity, and availability of information by protecting cyber assets from threats such as disclosure / exposure, tampering / destruction, and delay / disaster. The three elements of cyber security are:



- Confidentiality : The inability to obtain information in an unauthorized manner.
- Integrity : To protect data or resources from unauthorized changes
- Availability : Requirements for availability of an information system when an authorized user requires information or services.