KR Maritime Cyber Security

News from KOREAN REGISTER

Jan 2019

Vol. 009

KR Cyber Security Activities

● Organized reorganization to foster technologies related to 4th industry

President Lee, Jeong-kie of Korean Register(KR) said that KR reorganized its organization to make digital priority and establish an active response system for the organization. The core of this reorganization is to consolidate related organizations and to set up the control tower to increase efficiency of work in order to quickly become a digital priority. Specifically, 'Digital Technology Institute', which is a specialized organization consisting of Digitalization Team, ICT Solution Team, cyber Certification Team, and Information Technology team, was established.

Furthermore, Strategic and Planning Division and Administrative Division were integrated into Administrative Planning Division for the organic operation of the planning and management system. In need of systematic management of diverse and extensive technical fields, a separate R&D Division was established and R&D Center in Technical Division moved to Ship & Offshore R&D Center in R&D Division and Digital Technology Center added to R&D Division.

Korean Register has been researching core technologies for cyber security since 2016 by organizing a TFT for cyber security response and are providing cyber security technical services and certification services to shipping companies by establishing certification system for maritime cyber security system in 2018. The newly established Cyber Certification Team is currently in charge of cyber security certification for ships and companies and type approval for cyber security equipment and is developing a penetration test diagnostic tool that can be applied to Operating Technology (OT) systems. The details may be founded in KR homepage..

● Technical Seminar for Shipping Companies in Singapore

In December 2018, the Cyber Certification Team visited major shipping companies in Singapore and held a technical seminar on the latest trends in cyber security. IMO plans to force this practice in 2021 and the maritime business has already included cyber security management items in the shipper's inspection such as OCMIF TMSA and SIRE, RIGHTSHIP, etc. starting from 2018.

As the seminar was held at a time of high interest in the shipping industry, it was very well received by shipping companies and KR will provide cyber security guidelines through technical services and certification.

Since Last March, Cyber Certification Team in KR has successfully supported the establishment of cyber security management system of a shipping company by providing cyber security technology services, including advanced inspection for preliminary TMSA/SIRE inspection, improvement guidelines, cyber security training for employees, and utilization of PC security vulnerability diagnosis program.

Microsoft 2019 First Patch Release

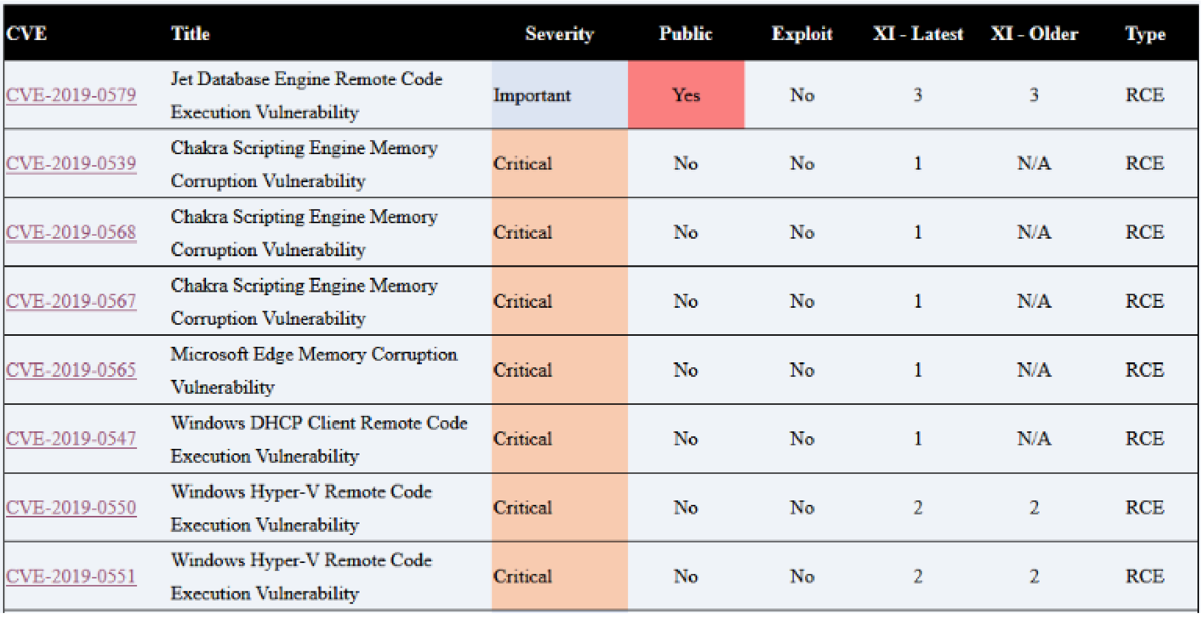
- **Microsoft, January 2019 Patch fixed 50 vulnerabilities**

Microsoft patched 50 vulnerabilities for 9 products (Windows OS, Internet Explorer, Microsoft Edge, ChakraCore, .NET Framework, ASP.NET, Microsoft Visual Studio, Microsoft Exchange Server, Microsoft Office).

In particular, in this patch, 17 bugs appeared as “remote code execution (REC)” that vulnerabilities allows attackers to execute code within Microsoft products or Windows components.

The vulnerability disclosed before the patch is CVE-2019-0579, which received the second highest rating, ‘Important’. The vulnerabilities is found in Windows jet database engine, which enables code execution remotely if successfully implemented. Exploitation should require the user to open a specially crated file.

Another critical vulnerability is CVE-2019-0547, which enables an attacker to execute arbitrary code on a Windows DHCP client machine. It requires specially crafted DHCP responses. Because the Windows DHCP client is available on all windows operating systems and vulnerabilities can be exploited remotely, uses should not miss this month’s update.



CVE	Title	Severity	Public	Exploit	XI - Latest	XI - Older	Type
CVE-2019-0579	Jet Database Engine Remote Code Execution Vulnerability	Important	Yes	No	3	3	RCE
CVE-2019-0539	Chakra Scripting Engine Memory Corruption Vulnerability	Critical	No	No	1	N/A	RCE
CVE-2019-0568	Chakra Scripting Engine Memory Corruption Vulnerability	Critical	No	No	1	N/A	RCE
CVE-2019-0567	Chakra Scripting Engine Memory Corruption Vulnerability	Critical	No	No	1	N/A	RCE
CVE-2019-0565	Microsoft Edge Memory Corruption Vulnerability	Critical	No	No	1	N/A	RCE
CVE-2019-0547	Windows DHCP Client Remote Code Execution Vulnerability	Critical	No	No	1	N/A	RCE
CVE-2019-0550	Windows Hyper-V Remote Code Execution Vulnerability	Critical	No	No	2	2	RCE
CVE-2019-0551	Windows Hyper-V Remote Code Execution Vulnerability	Critical	No	No	2	2	RCE

Ref. : Microsoft January 2019 Patch Tuesday fixes 50 vulnerabilities

Cybersecurity Issues and Countermeasures of Ship and Marine

● Cybersecurity Issues of Ship and Marine

According to a recent document released by the international shipping industry, 'Guidelines on Cyber Security on Board Ships (Rev.3), ships face the same type of cybersecurity issues as other IT systems. This document contains rules and guidelines for securing ship IT/OT systems and provides examples of what happens when the correct procedures are not followed. This is a case of cyber security incidents that occurred on ships and harbors in the past and has not been publicly disclosed.

<Case 1> ECDIS was infected with the virus

A new-build dry bulk carrier was delayed for several days after ECDIS was infected with the virus. The ship did not have a paper chart. A producer technician was required to visit the ship and, after spending a significant time in troubleshooting, discovered that both ECDIS networks were infected with a virus. The source and means of infection in this case are unknown. The delay in sailing and costs in repairs totaled in the hundreds of thousands of dollars (US).

<Case 2> Ship's ransomware infection

A shipowner reported that the company's business networks were infected with ransomware, apparently from an email attachment. The source of the ransomware was from two unwitting ship agents, in separate ports, and on separate occasions. Ships were also affected but the damage was limited to the business networks, while navigation and ship operations were unaffected. In one case, the owner paid the ransom.

<Case 3> Cyber incident caused by not set up proper RDP(Remote Desktop Protocol) passwords.

A ransomware infection on the main application server of the ship caused complete disruption of the IT infrastructure. The ransomware encrypted every critical file on the server and as a result, sensitive data were lost, and applications needed for ship's administrative operations were unusable. The incident was reoccurring even after complete restoration of the application server. The root cause of the infection was poor password policy that allowed attackers to brute force remote management services successfully. The company's IT department deactivated the undocumented user and enforced a strong password policy on the ship's systems to remediate the incident.

Ref. : Ships infected with ransomware, USB malware, worms

The report includes details of two incidents where USB thumb drives have led to a cyber-security incident, delays, and financial damage.

<Case 1>

A dry bulk ship in port had just completed bunkering operations. The bunker surveyor boarded the ship and requested permission to access a computer in the engine control room to print documents for signature. The surveyor inserted a USB drive into the computer and unwittingly introduced malware onto the ship's administrative network. The malware went undetected until a cyber assessment was conducted on the ship later, and after the crew had reported a "computer issue" affecting the business networks. This emphasises the need for procedures to prevent or restrict the use of USB devices onboard, including those belonging to visitors.

<Case 2>

A ship was equipped with a power management system that could be connected to the internet for software updates and patching, remote diagnostics, data collection, and remote operation. The company's IT department made the decision to visit the ship and performed vulnerability scans to determine if the system had evidence of infection and to determine if it was safe to connect. The team discovered a dormant worm that could have activated itself once the system was connected to the internet and this would have had severe consequences. The shipowner stated that before the discovery, a service technician had been aboard the ship. It was believed that the infection could potentially have been caused by the technician. The worm spread via USB devices into a running process, which executes a program into the memory.

With the continued increase in cyber attacks on shipping and maritime industrial facilities, many related companies are looking for ways to respond to these threats. It is used for many purposes, such as software patches, ECIDS updates, and moving documents between systems, but it also infects malicious code such as ransomware through USB and attacks systems that actually operate. There are many attack techniques that circumvent even the introduction of security solutions, such as only USB connections that are certified for USB security.

In response, penetration testing consulting is conducted to determine how much USB penetration is possible, and cyber criminals use the USB to obtain intelligence in advance about how malware or attacks are distributed and where the target is located and what type of facility or company they become, and introduce the Cyber Threat Intelligence Service (CTI). At the same time, cyber security training is essential to how easily attacked, infected, and impacted and damaged internal staff. No matter how much penetration testing is conducted and security solutions are introduced, all security becomes useless if internal employees attempt to connect to infected USB.

Understanding of Cyber Threat(OWASP Top 10)

● Understanding of cyber threat

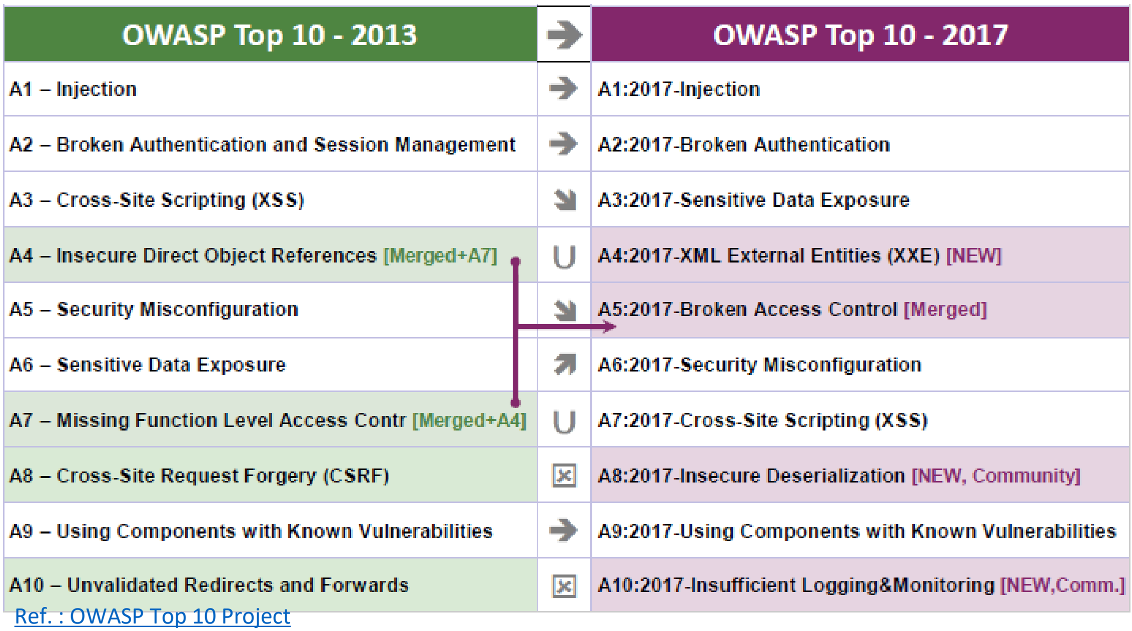
A Cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction,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

Open Web Application Security Project (OWASP) is an open source web application security project, mainly researching web exposure, malicious files and scripts, security vulnerabilities. OWASP Top 10, which is frequently used and can give significant impact among web application vulnerabilities, are published in 2004, 2007 , 2010, 2013 and 2017, In this newsletter we would like to analyze the each of OWASP Top 10.



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.]

Ref. : OWASP Top 10 Project

- **OWASP Top 10 -2017**

OWASP Top 10 project was aimed at raising security awareness among developers and administrators, but it is now becoming the industry standard for application security. Beyond the Top 10, there are many threats to web application security, and the Top 10 threats are constantly changing. A4, A8, A10 items were newly added IN 2017, and A4, A7 items were merged to A5 in 2017.

OWASP Top 10	Details
A1 : Injection	SQL, OS, XXE, LDAP injection, untrusted data is delivered as part of an instruction or query statement, causing unexpected commands to be executed or accessing data without proper authorization
A2 : Broken Authentication	Incorrect implementation of application functions related to authentication and session management vulnerability allowing an attacker to compromise a password, key, or session token, or to exploit another implementation vulnerability
A3 : Sensitive Data Exposure	Many web applications and APIs are vulnerabilities that do not properly protect sensitive information such as financial information, and personally identifiable information
A4 : XML External Entities (XXE)	Vulnerability in evaluating external entity references within XML documents - External objects can expose internal files using file URI handlers, internal file shares, remote code execution
A5 : Broken Access Control	A vulnerability that does not properly enforce restrictions on what an authenticated user can perform
A6 : Security Misconfiguration	A result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information.
A7 : Cross-Site Scripting (XSS)	Vulnerability in which an application takes untrusted data and sends it to a web browser without proper validation or escaping, resulting in user session hijacking, deface web sites, or redirect the user to malicious sites.
A8 : Insecure Deserialization	Vulnerability that could allow remote code execution due to insecure deserialization to cause elevation attacks, injection attacks, and replay attacks
A9 : Components with Known Vulnerabilities	Vulnerability that results in data loss or server compromise due to components such as libraries, frameworks, and other software modules that have known vulnerabilities
A10 : Insufficient Logging & Monitoring	Vulnerability in data tampering, extraction, and tampering due to insufficient logging and monitoring

Guidelines of Data Security Policies

- **The need for establishing data security policies**

Data security policies need to be established because leakage or corruption of company confidential information by cyber attacks can undermine business continuity, including financial loss, reputation, and productivity degradation. The company shall establish and operate a data backup plan necessary for system operation and restoration to minimize damage caused by system failure, data corruption, etc. and shall perform backups on a regular or necessary basis in accordance with the backup plan. In addition, the company shall encrypt and store data with a security grade higher than the confidentiality grade according to the designated security class.

- **KR Guidance for Maritime Cybersecurity Management System requirement (CSMS1)**

Data Backup(210.1) : Important data should be backed up in a separate space and stored securely.

Data Access Control(210.2) : Data should be limited in user access according to its importance, and physical and logical access control should be performed.

Communication Encryption(216.1) : An environment in which data can be communicated in an encrypted manner should be established.

Data Encryption(216.3) : Data classified as important must be encrypted and stored.

- **Backup policy (Example)**

Server	Backup requirement								
	Category	**Form**	**Type**	**Capacity**	**Period**	**Storage**	**RTO**	**Media**	**Method**
DB server 01	OS and main file	File system	Online	12GB	Monthly	3 days	1 hour	DAT	Manual
	DBMS	File system	Online	30GB	Monthly	3 days	2 hours	DAT	Auto
	DB data	RAWDevice	Online	120GB	Monthly	3 days	2 hours	DAT	Auto
	DB log data	File system	Online	12GB	Daily	3 days	1 hour	DAT	Auto
DB server 02	OS and main file	File system	Online	12GB	Monthly	3 days	1 hour	DAT	Manual
	System engine	File system	Online	30GB	Monthly	4 weeks	2 hours	LTO	Auto
	User file	File system	Online	30GB	Daily	1 week	1 hour	LTO	Auto

- **Data encryption criteria (Example)**

Rating	Classification	Description	Example	Encryption
1st	Confidential	Data provided only to certain authorized employees in the company	Contract Status Confidential cargo loading status	O
2nd	Internal	Data is available to employees in the company, but limited to outsiders	Vessel navigation route Cargo Status	X
3rd	General	Data that are open to everyone, including internal and external employees, customers	Company introduction Company disclosure data	X

- **Encryption application by category (Example)**

Application	Classification	Example	Encryption example	Recommendation algorithm* (Password strength)
Store	When encrypted information cannot be decrypted	Password	Hash algorithm	SHA-224/256/384/512
	When it is necessary to be able to decrypt encrypted information	Confidential document	Symmetric key encryption Public key encryption	AES(AES-128/192/256), TEDA, ARIA, SEED
Transmission	Encryption to prevent leakage of information to third parties during transmission	Confidential document Password	Communication channel encryption	SSL/TLS

- **Encryption method for each application or medium (Example)**

Category	Application of encryption
Database	Encrypt data, such as confidential data, using a dedicated program or management system for database security
PC	Utilizing the encryption program (ex: DRM program) introduced by the company or using the password function provided by the operating system, office program, and compression program
Portable storage media	Use the encryption provided by the storage media itself or save each file encrypted in the absence of security
E-mail	Use of email security protocols such as S/MIME (Security Services for Multipurpose), or password encryption provided by the file / disk password program if the mail encryption program is not provided
Messenger	Messenger provides conversation and file transfer encryption that is provided by itself, and provides an encrypted file in advance when the function is not provided

Explanation of Term

- **CVE(Common Vulnerabilities and Exposures) :** CVE is a dictionary of publicly disclosed cybersecurity vulnerabilities and exposures that is free to search, use, and incorporate into products and services, per the terms of use. The CVE List is built by CVE Numbering Authorities (CNAs). Every CVE Entry added to the list is assigned by a CNA.

  (Eg) CVE-2018-0001 : First identified vulnerability in 2018

- **SHA(Secure Hash Algorithm) :** Secure hash algorithm and next versions of SHA-1 and SHA-2 are government standard hash functions developed by National Institute of Standards and Technology (NIST). Hash means converting random data into fixed data sizes. The hash algorithm specifies how to hash, and SHA-256 is a hash algorithm that converts random input data into 256 bits of output data. SHA-1 was used with a number of security protocols, including TLS, SSL, SSH, IPSec, but recently the SHA-1 algorithm's weakness was exposed by a cryptographic attack.

- **AES(Advanced Encryption Standard) :** The National Institute of Standards and Technology (NIST) published the AES as the U.S. Federal Information Processing Standard (FIPS-197) in 2001. As this is a representative symmetric key cryptography algorithm, send and receivers use the same key for encryption and redundancy. The AES algorithm secures the input plain to 128 bits in length, and allows the user to choose between 128-bit, 192-bit, and 256-bit encryption keys. So far, attacks on known block cipher algorithms have been safely designed.

- **SSL(Secure Sockets Layer):** A cryptographic protocol developed by Netscape that protects communication between the web server and the web browser. SSL is a session-oriented protocol that guarantees confidentiality and integrity by protecting not only the web, e-mail, FTP, but also Telnet traffic.

- **TLS(Transport Layer Security):** An Internet standard web security protocol built on SSLv3. Works the same way as SSL, but uses stronger authentication and encryption protocols.