C C S Technical Information

(2021) Technical Information No.10 Total No.516
Jun.07,2021
(Total 7 pages)

To: Ship Owners, Ship Management Companies, CCS branches, Surveyors and Auditors

Cyber Security Warning Information on the Prevention of Ransomware Cyber-attack

Recently, the ransomware cyber-attack was deeply focused on by the industry. On May 7, a U.S. fuel pipeline company was attacked by a ransomware virus, and forced to suspend oil delivery business, which had a serious impact on the U.S. fuel supply. On May 9, Tulsa was also attacked by the ransomware virus, which led to the shutdown of its internal systems and services. On May 17, the Irish Health Service Executive (HSE) announced that it had suffered a major ransomware attack. These attacks have brought great impact on the local economy and living.

Ransomware usually uses strong encryption technology, which can cause files unreadable, data corrupted and computers locked. According to the statistics, Darkside, Crysis, Phobos, Globeimposter, Maze, Conti and Babuk Locker are the major active ransomware in recent, with the main features to be shown in the table below:

Ransomware	**Main characteristics**
Darkside	Mainly for the Windows system, but there are also variants for the Linux system. A large number of penetration testing tools are used to perform vulnerability scanning and intrusion penetration to the external network systems of relevant organizations. After entering the internal network, they target Windows Domain Server.
Crysis Phobos GlobeImposter	Attempt to obtain a remote desktop login password by brute force attack, and log on to the user's machine after obtaining the remote desktop password to manually load the ransomware.
Maze	It mainly tempts users to download the attachment of email by disguising as tax mails and then encrypt system files.
Babuk Locker	Advanced Persistent Threat (APT) attacks are used against target users in a variety of ways.

The ways of ransomware transmission are becoming more and more diverse, mainly in the following ways.

1. Website embedded trojan. When users browse websites with trojan virus, the computer terminal is likely to be infected with virus.
2. E-mail. Using the current hot keywords such as epidemic prevention, vaccine and so on, attackers send spam and phishing e-mail on the Internet. Once the recipient clicks on the link or attachment with the virus, it will cause the virus to run.
3. Vulnerability. Attackers use system, device port protocol and other vulnerabilities to penetrate and infect computers in the local network. Among them, the vulnerabilities of remote desktop and shared folder port are still the most common way to complete the intrusion penetration.
4. Software embedding. Attackers bind ransomware with other software, especially pirated software, illegally cracked software, and activation tools, so as the user download and install, and then their computer shall be infected.
5. Storage medium. The attacker uses U disk, CD and other media to spread the ransomware through implantation or cross infection.
6. social engineering. Attackers use social engineering to obtain information for horizontal penetration. The target of social engineering attack is personnel, and most of them use deception, induction and other ways

In order to prevent the cyber-attack of ransomware, CCS suggests that the ship owners and the ship management companies should develop network security strategy and network security emergency response plan, to guide employees to use the network safely, establish network security defense barriers, and strengthen staff network security awareness and knowledge training. On the other hand, more attention should be paid to the threat information, the timely troubleshoot and the repair system vulnerabilities, and the following protective measures should be taken:

1. To strengthen the company and ship internet port management, and close the ports that are not often used on computers and servers, such as 445, 135, 137, 138, 139, 3389, 5900, etc.
2. To list assets and remove unused assets, regularly make a backup of the important data and files in different places or machines, and make disaster recovery for important systems;
3. To reinforce network security, check the safety equipment regularly.
4. To take necessary measures to strengthen the security protection of the computer system, carry out vulnerability scanning and risk assessment regularly, update and upgrade the system and application in time, and repair the existing medium and high risk vulnerabilities.

5. To standardize the use of storage media such as the flash drive/USB media, mobile hard disk and CD, do not use/open the flash drive/USB media, CD, E-mail, web links and files from unknown sources.
6. To strengthen password complexity, instead of using weak password.
7. To purchase software and APPs through official store, and do not download and install pirated software, illegally cracked software and activation tools online.
8. To avoid mapping RDP services directly to the external network and using default ports.
9. To maintain other routine measures concerning cyber security, and pay attention to relevant guidelines on website of IMO, IACS and CCS, etc timely.

The shipowners and shipping management companies concerned are invited to pay attention to the contents of this Notice.

This Notice is published on the CCS website (www.ccs.org.cn) and will be transmitted to relevant shipowners and shipping management companies by each CCS Branch within its jurisdiction area.

If you have any inquiry， Please contact the following persons in charge without hesitation:
Science & Technology Innovation and Test Center of CCS
Zhang Xuanwu, Tel: (+86) 10-5811 3439 / 19520307720
Email: zhangxuanwu@ccs.org.cn
Deng Linyi, Tel: (+86) 10-5811 2320 / 15010318271
Email: lydeng@ccs.org.cn

Attachment: vulnerabilities

1. AMD

CVE ID	CVE-2020-12967 CVE-2021-26311	time	2021-05-17
type	Code execution	level	high risk
Vulnerability details	CVE-2020-12967: This vulnerability is caused by lack of nested page table protection in AMD SEV/SEV-ES functionality and can cause arbitrary code execution in the Guest VM if an attacker has permission to corrupt the server hypervisor. CVE-2021-26311: This vulnerability exists in AMD SEV/SEV-ES functionality. According to this security announcement, memory can be rearranged in the Guest address space that is not detected by the authentication mechanism, and if an attacker has permission to corrupt the server hypervisor, this vulnerability can be used to implement arbitrary code execution in the Guest VM.		
Scope	This vulnerability affects all AMD EPYC^{TM}processors (1st / 2nd / 3rd generation AMD EPYC^{TM} processors and AMD EPYC^{TM} embedded processors)		
The disposal of advice	AMD has now fixed this vulnerability with the SEV-SNP feature, but this feature is only supported in the 3rd generation AMD EPYC^{TM}. It is recommended that 3rd generation AMD EPYC^{TM} users implement the SEV-SNP feature as soon as possible.		

2. VMware

CVE ID	CVE-2021-21984	time	The 2021-05-6
type	Remote code execution	level	serious
Vulnerability details	Due to the unauthorized VAMI API, an attacker can exploit this vulnerability by upgrading the API through the management interface (VAMI) to gain access to the VRealize Business for Cloud virtual appliance and execute code remotely without authentication or user interaction.		
scope	VMware vRealize Business for Cloud< 7.6.0		
The disposal of advice	The vRealize Business for Cloud 7.6 security patch ISO file is recommended to download and apply as soon as possible.		

CVE ID	CVE-2021-28550	time	2021-05-11

	CVE-2021-28562 CVE-2021-28553		
type	Remote code execution	level	high risk
Vulnerability details	An attacker can use it to install malware on a target system or to take over a computer.		
scope	Adobe Acrobat Reader		
The disposal of advice	It is recommended to install the latest patch as soon as possible.		

3. Cisco

CVE ID	CVE-2021-1402 CVE-2021-1445 CVE-2021-1504 CVE-2021-1448 CVE-2021-1493 CVE-2021-1501	time	The 2021-4-28
type	DDOS, command injection, buffer overflow	level	At high risk of
Vulnerability details	CVE-2021-1402: A denial-of-service vulnerability exists in Cisco FTD's software-based SSL/TLS message handler due to insufficient validation of SSL/TLS messages when devices perform software-based SSL decryption. CVE-2021-1445, CVE-2021-1504: Multiple denial-of-service vulnerabilities exist in Cisco ASA and FTD due to lack of proper input validation for HTTPS requests. CVE-2021-1448: A command injection vulnerability exists in the CLI of Cisco FTD due to insufficient validation of user-supplied command parameters. CVE-2021-1493: A buffer overflow vulnerability exists in the Web services interfaces of Cisco ASA and FTD due to insufficient boundary checking of specific data provided to the Web services interfaces of the affected systems. CVE-2021-1501: Denial of service vulnerability in SIP check engine of Cisco ASA and FTD due to crash during hash query of SIP pinhole connection.		
scope	Cisco Adaptive Security Device (ASA) and Firepower Threat Defense (FTD)		
The disposal of advice	Cisco has issued security updates for Cisco ASA and FTD. We recommend timely repair or upgrade according to the security notice issued by the		

	authorities.

4. Linux

CVE ID	CVE-2020-28588	time	The 2021-4-28
type	Information disclosure	level	high risk
Vulnerability details	The vulnerability exists in the /proc/pid/syscall function of 32-bit ARM devices running Linux. Due to the incorrect conversion between numeric types, an attacker can exploit the vulnerability by reading the file/proc/<pid>/syscall to view kernel stack memory information or use this vulnerability to exploit other unfixed Linux vulnerabilities. In addition, attackers can also bypass KASLR through this information disclosure vulnerability. Randomization (KASLR) is an anti-use technique that randomly places various objects to prevent guesswork by an attacker.		
scope	V5.1 - rc4 - v5.10 - rc4 Tested version: The Linux Kernel v5.10 - rc4 The Linux Kernel v5.4.66 The Linux Kernel v5.9.8		
The disposal of advice	Upgrade to the latest version is recommended.		

5. Apache

CVE ID	CVE-2021-29200 CVE-2021-30128	time	The 2021-4-28
type	Remote code execution, deserialization	level	At high risk of
Vulnerability details	Because the use of RMI (Remote Method Invocation) leads to unsafe deserialization, an unauthenticated attacker can execute code remotely by exploiting this vulnerability.		
scope	Version of Apache OFBiz prior to 17.12.07		
The disposal of advice	It is recommended to upgrade to Apache OFBiz 17.12.07 or later.		
CVE ID	CVE-2021-27850	time	The 2021-4-14
type	Remote code execution	level	serious
Vulnerability details	An attacker does not need to be authenticated to exploit it. The vulnerability bypasses the CVE-2019-0195 fix		
scope	Apache Tapestry 5.4.5 Apache Tapestry 5.5.0		

	Apache Tapestry 5.6.2 Apache Tapestry 5.7.0
The disposal of advice	This vulnerability has been officially fixed, and it is recommended to upgrade to the following versions: Apache Tapestry 5.4.0-5.6.2, upgrade to 5.6.2 or later. Apache Tapestry 5.7.0, upgrade to 5.7.1 or later.

6. Oracle

CVE ID	CVE-2021-2135 CVE-2021-2136 CVE-2021-2157	time	The 2021-4-21
type	Unauthorized access	level	high risk
Vulnerability details	CVE-2021-2135: An unauthenticated attacker can send a malicious request via the T3 or IIOP protocol, ultimately taking control of the server. This vulnerability can be exploited without user interaction. CVE-2021-2136: An unauthenticated attacker can send malicious requests over the IIOP protocol and ultimately take control of the server. This vulnerability can be exploited without user interaction. CVE-2021-2157: An unauthenticated attacker can send a malicious request over HTTP and ultimately gain unauthorized access to critical data. This vulnerability can be exploited without user interaction.		
scope	Oracle WebLogic Server 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0		
The disposal of advice	At present, Oracle has issued the relevant security patch, it is recommended to install as soon as possible.		

CVE ID		time	The 2021-4-19
type	Remote code execution	level	At high risk of
Vulnerability details	WebLogic has been revealed to have a T3 protocol deserialization 0day vulnerability, which can be exploited by an attacker to cause remote code execution. The vulnerability is currently in the open 0day state and the POC /EXP has been made public on GitHub. In the poc of the vulnerability, the java.rmi MarshalledObject class is used, and the objBytes property is used as a deserialized stream from which the object can be parsed and weblogic blacklisting can be bypassed by replacing the objBytes with the specified deserialization.		
scope	Oracle WebLogic Server 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0		
The disposal of advice	It is recommended to upgrade the JDK to the latest version and disable the IIOP/T3 protocol as a temporary mitigation measure.		