C C S Technical Information

(2020) Technical Information No.62 Total No.496
Nov.03,2020
(Total 2 + 6 pages)

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

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

With the digitalization of the shipping industry, which is slow to respond to cyber threats, has become a priority target of cyber-criminal organizations under the impetus of epidemic situation and interests. Statistically, the number of cyber-attacks on the shipping industry has increased by 400 percent since February this year. On August 15, 2020, the world's leading cruise company was attacked by ransomware. The attackers encrypted part of the information technology system and stole some documents. On September 28, a ransomware attack on the information systems of a container shipping company has disrupted services at its offices in Shanghai and elsewhere in China, forcing it to shut down network services and process business orders manually, while the website of the International Maritime Organization (IMO), a UN agency, was hit by a cyber-attack three days later, making its public website and other web-based services unavailable on that day.

According to the cyber threat intelligence analysis, ransomware is turning to deploying malicious code by purchasing network access and infiltrating target systems that have been leaked, which speeds up the attack process and enables cyber criminals to achieve their goals faster and more effectively. Therefore, CCS recommends that shipowners and ship management companies pay attention to threat intelligence, investigate and repair system vulnerabilities in a timely manner, improve defense capabilities to reduce risks, and take the following preventive measures.

1. Pay more attention to the staff safety knowledge training.
2. The network should be cut off in time, after the ransomware invasion, and contact the security department or the company for emergency treatment at the first time.
3. Update and patch the system and each service component in time.
4. Deploy security devices at network boundaries, such as firewalls, IDS, mail gateways, etc.
5. Do not believe network messages, do not browse bad websites, do not open email attachments, do not run executable programs at will.
6. Clear the role access permissions of each server and reasonably set the access permissions

of server-side files.

7. Timely backup data and ensure data security. Control data access rights strictly.
8. Do other routine safety related tasks, pay attention to relevant guidelines on website of IMO, IACS and CCS.

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.

Please contact Science & Technology Innovation and Test Center of CCS for any inquiry in the implementation as follows:
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

Company	CVE ID	Vulnerability Description	Affected Software	Suggestion
Microsoft	CVE-2020-16898 CVE-2020-16919 CVE-2020-16897 CVE-2020-16914 CVE-2020-16921 CVE-2020-16930 CVE-2020-16933 CVE-2020-16938 CVE-2020-16947 CVE-2020-16955	These vulnerabilities are remote code execution vulnerabilities, existing in Excel, Outlook, Windows graphics components, and Windows TCP/IP stack. Among them, CVE-2020-16898 exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. An attacker who successfully exploited this vulnerability could gain the ability to execute code on the target server or client.	Windows 10 Version1709, Version1803, Version1809, Version1903, Version1909, Version2004， Windows Server 2019， Windows Server 2019 (Server Core installation)， Windows Server version 1903 (Server Core installation), version 1909 (Server Core installation), version 2004 (Server Core installation)	Download and install the official update patches.
	CVE-2020-17022	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code.	Windows 10 Version 1709, Version 1803, Version 1809, Version 1903, Version 1909, Version 2004	1. Download and install the official update patches. 2. Mitigate the risk by disabling ICMPv6 RDNSS.

	CVE-2020-17023	A remote code execution vulnerability exists in Visual Studio Code when a user is tricked into opening a malicious 'package.json' file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Visual Studio Code prior to version 1.50.1	
Adobe Creative Cloud Desktop Application	CVE-2020-24422	The vulnerability could lead to arbitrary code execution.	Creative Cloud Desktop Application prior to version 5.3 (old installer) and version 2.2 (new installer)	Upgrade to the latest version.
Adobe InDesign	CVE-2020-24421		Adobe InDesign prior to version 16.0	
Adobe Media Encoder	CVE-2020-24423		Adobe Media Encoder prior to version 14.5	
Adobe Premiere Pro	CVE-2020-24424		Adobe Premiere Pro prior to version 14.5	
Adobe Photoshop	CVE-2020-24420		Photoshop prior to version 21.2.3	
Adobe After Effects	CVE-2020-24418 CVE-2020-24419		Adobe After Effects prior to version 17.1.3	

Adobe Animate	CVE-2020-9747 CVE-2020-9748 CVE-2020-9749 CVE-2020-9750		Adobe Animate prior to version 21.0	
Adobe Marketo	CVE-2020-24416	The vulnerability is a cross-site scripting (XSS) vulnerability that can lead to arbitrary execution of JavaScript scripts in the browser.	Marketo Sales Insight Salesforce prior to version 1.4357	
Adobe Dreamweaver	CVE-2020-24425	The vulnerability could result in increased permissions for the current logged-in user.	Adobe Dreamweaver prior to version 21.0	
Adobe Illustrator	CVE-2020-24409 CVE-2020-24410 CVE-2020-24411 CVE-2020-24412 CVE-2020-24413 CVE-2020-24414 CVE-2020-24415	The vulnerability could lead to arbitrary code execution.	Illustrator 2020 prior to version 25.0	

Cisco	CVE-2020-3554 CVE-2020-3373 CVE-2020-3528 CVE-2020-3529 CVE-2020-3572 CVE-2020-3304 CVE-2020-3436 CVE-2020-3456 CVE-2020-3562 CVE-2020-3571 CVE-2020-3550 CVE-2020-3549 CVE-2020-3410 CVE-2020-3499 CVE-2020-3577 CVE-2020-3514 CVE-2020-3533 CVE-2020-3563	18 Cisco Security Advisories that describe vulnerabilities in Cisco ASA, FMC, and FTD Software. Some serious vulnerabilities are as follows: A vulnerability (CVE-2020-3456) in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A vulnerability (CVE-2020-3499) in the licensing service of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper handling of system resource values by the affected system. An attacker could exploit this vulnerability by sending malicious requests to the targeted system. A vulnerability (CVE-2020-3563) in the packet processing functionality of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of TCP packets to a specific port on an affected device.	Firepower 2100 series in the ASA facility in non-appliance mode, Firepower 4100 series facilities, Firepower 9300 series facilities Cisco FMC running on any Cisco device that is connected to the license, FTD 6.2.3 and earlier version, FTD 6.3.0 – FTD 6.6.0	Refer to the official repair suggestions to upgrade to the safe version in time.

Apache Kylin	CVE-2020-13937	Kylin has one restful api which exposed Kylin's configuration information without any authentication, so it is dangerous because some confidential information entries will be disclosed to everyone.	Kylin2.0.0, 2.1.0, 2.2.0, 2.3.0, 2.3.1, 2.3.2, 2.4.0, 2.4.1, 2.5.0, 2.5.1, 2.5.2, 2.6.0, 2.6.1, 2.6.2, 2.6.3, 2.6.4, 2.6.5, 2.6.6，Kylin3.0.0-alpha, 3.0.0-alpha2, 3.0.0-beta, 3.0.0, 3.0.1, 3.0.2, 3.1.0，Kylin4.0.0-alpha	The Apache Kylin team has released a new version and it is recommended to upgrade to 3.1.1 in time.
Oracle	CVE-2020-14820 CVE-2020-14825 CVE-2020-14841 CVE-2020-14859 CVE-2020-14882	These vulnerabilities allow an unauthenticated attacker to send constructed malicious requests over HTTP IIOP T3 to execute code in Oracle WebLogic Server.	Oracle WebLogic Server 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	Refer to the official repair suggestions to upgrade to the safe version in time.
Mozilla	CVE-2020-15969 CVE-2020-15254 CVE-2020-15680 CVE-2020-15681 CVE-2020-15682 CVE-2020-15683 CVE-2020-15684	These vulnerabilities could allow for arbitrary code execution. Depending on the user's permissions, an attacker can install programs to view, change, delete, or create data, and the greater the user's permissions, the greater the impact.	Mozilla Firefox prior to version 82	Upgrade to the latest version.
Rapid7	CVE-2020-7363 CVE-2020-7364 CVE TBD-Opera CVE-2020-9987	These vulnerabilities allow attackers to trick users into accessing malicious sites while showing the incorrect URL in the address bar.	UC browser 13.0.8，IOS 13.6，Opera Touch 2.4.4，Opera Mini 51.0.2254	Upgrade to the latest version.

Google	CVE-2020-15999	The vulnerability, a memory corruption vulnerability in the FreeType font rendering library of the standard Chrome distribution, has been exploited to attack users.	Chrome prior to version 86.0.4240.111	download and install the official patch or upgrade to Chrome 86.0.4240.111.
IBM	CVE-2020-4414	A memory leak vulnerability in IBM Db2 relational database could allow an attacker to gain access to sensitive data or cause a denial-of-service (DoS) condition in the database.	IBM Db2 versions for Linux, UNIX, and Windows (9.7, 10.1, 10.5, 11.1, 11.5)	Download and install the officially released patch.