U.S. MARITIME ADVISORY 2024-002
Threat Type: Foreign Adversarial Technological, Physical, and Cyber Influence
Geographic Area: Worldwide

This revised advisory cancels U.S. Maritime Advisory 2023-009

1. Issue: This Advisory seeks to alert maritime stakeholders of potential vulnerabilities to maritime port equipment, networks, operating systems, software, and infrastructure. Foreign companies manufacture, install, and maintain port equipment that creates vulnerabilities to global maritime infrastructure information technology (IT) and operational technology (OT) systems. In the past few years, the U.S. Government has published several documents (see paragraph 4 below) illuminating the risks associated with integrating and utilizing the People's Republic of China's (PRC's) state-supported National Public Information Platform for Transportation and Logistics (LOGINK), Nuctech scanners, and automated ship-to-shore cranes worldwide.

LOGINK is a single-window logistics management platform that aggregates logistics data from various sources, including domestic and foreign ports, foreign logistics networks, shippers, shipping companies, other public databases, and hundreds of thousands of users in the PRC. The LOGINK logistics platform, which was first marketed outside of the PRC in 2010, was developed by the PRC Ministry of Transport. At least 24 global ports have cooperation agreements with LOGINK, which can collect massive amounts of sensitive business and foreign government data, such as corporate registries and vessel/cargo data. The PRC government is promoting logistics data standards that support LOGINK's widespread use, and LOGINK's installation and utilization in critical port infrastructure very likely provides the PRC access to and/or collection of sensitive logistics data.

Nuctech Company, Ltd. (Nuctech) is a PRC State-controlled entity that manufactures and fields data-centric partially state-owned security inspection equipment at key logistic nodes worldwide. Nuctech equipment capabilities include x-ray, backscatter, and thermal platforms; explosives detection; non-intrusive products (such as baggage and parcel inspection (NIIE); Artificial Intelligence (AI); and facial cognition/recognition capabilities). Nuctech equipment access includes biometric information, personally identifiable information (PII), patterns of life cargo information, proprietary data, and geo-locational metadata. Several countries have raised concerns about the security risks posed by Nuctech equipment deployed in critical infrastructure given the company's control by the PRC government. The United States added Nuctech to the Department of Commerce's Entity List for its involvement in activities contrary to the national security interests of the United States. Specifically, the U.S. government determined Nuctech's lower performing equipment impairs U.S. efforts to counter illicit international trafficking in nuclear and other radioactive materials. Lower performing equipment means less stringent cargo screening, raising the risk of proliferation.

ZPMC (Shanghai Zhenhua Heavy Industries Company Limited) maintains the largest share, by sales revenue, of the ship-to-shore crane market worldwide. These cranes may, depending on their individual configurations, be controlled, serviced, and programmed from remote locations. These features potentially leave them vulnerable to exploitation.

2. Guidance: Maritime industry stakeholders, including vessel owners/operators, shippers, and port operators exposed to these risks should apply cybersecurity best practices for Access Control (identity and access management), vulnerability mitigation, and configuration management, and should:

- Position themselves to increase their cybersecurity and cyber resiliency to respond to and report any incidents that could inhibit their ability to continue operations.
- Maintain a comprehensive understanding of data sharing and network access permissions within contractual agreements.
- Stress to their personnel the importance of understanding and knowing who maintains access to maritime technology throughout any port or facility they utilize.
- Be wary of untrusted network traffic and treat all traffic transiting their networks – especially third-party traffic – as untrusted until it is validated as legitimate.
- Ensure infrastructure operational resiliency, regarding system security, as well as the ability to maintain equipment and sourcing for critical parts and upgrades.
- Maintain fully recoverable backups and practice recovery from backups.
- Partner with academia and government to develop and maintain optimal cybersecurity hygiene by participating in information sharing exchanges and cyber drills and exercises.

The below mitigation measures can be utilized to reduce the risks associated with automated port cranes:

- Improve segmentation between the crane and other port systems/networks to reduce an adversary's initial cyber access. Reduce unnecessary communications and network services between business and management networks and the crane network and disallow multi-homed systems across these networks.

- Utilize secure file transfer tools/maintain a secure file transfer to reduce the risk of malware when transferring files into the crane network, such as firmware updates, reducing dependency on removable media (e.g., USBs).

- Provide dedicated remote access systems and processes for crane devices which utilize and enforce Multifactor Authentication (MFA). Define formal policies and procedures for firewall rule changes needed to control access.

- Separate and segment crane management functions from crane operational systems to reduce cyber access by adversaries. Keep crane management functions (e.g., diagnostics, patching, programmable logic controller (PLC) program modification/updating) on

separate segments and restrict modifications from crane operational systems, including the on-board and remote crane management systems (RCMS).

- Monitor all communications on the crane network (all ingress and egress traffic), especially those between the crane and broader port operational and management systems. Monitor all communications paths used to connect to the crane, including from the RCMS remotely. Monitor host activities for operational management systems.

- Require vendor update completion through physical visits at crane operating sites whenever possible and discourage vendors from completing remote updates.

Verify the integrity and security of on-board crane devices and networks:

- Perform periodic integrity checks and validation of PLC application programs to ensure their correct/secure operation.

- Ensure on-board crane virtual local area network VLANs enforce segmentation of critical control devices. The VLANs should segment devices and communications supporting core control functions (e.g., PLCs, drives, I/O, etc.) from those used for non-critical functions (e.g., cameras, surveillance, etc.). Any devices from untrusted suppliers should also be segmented on a separate VLAN.

Maintain robust response and recovery programs to ensure key on-board crane systems and devices can be efficiently restored:

- Perform periodic backups of key software images and programs, including operating system images (crane management, cabin view, and ground view system), application programs for PLCs, and settings for other key devices (e.g., variable frequency drive (VFD) network switches). Make sure backups are stored offline. Periodically test backups and restoration procedures.

- Maintain spare hardware of key components, including PLCs, embedded/small form factor computers, and network devices. Ensure the organization has procedures for performing and testing hardware rebuilds.

Ensure strong physical security and access control of devices and infrastructure used to operate and manage the crane:

- Ensure ground facilities used to support crane operations, including data closets, server rooms, and operator workstations, have appropriate physical security controls.

- Keep on-board devices such as PLCs, networking devices, and computers within locked data cabinets.

3. Contact Information: Maritime stakeholders who discover compromised equipment or suspicious activity within the Marine Transportation System (MTS), or OT/IT assets should contact:

- U.S. Coast Guard National Response Center: 1-800-424-8802
- U.S. Coast Guard Cyber Command (CGCYBER), Maritime Cyber Readiness Branch (MCRB): maritimecyber@uscg.mil
- Cybersecurity and Infrastructure Security Agency (CISA) Central: 888-282-0870 or central@cisa.gov
- FBI's Cyber Division: 855-292-3937 or CyWatch@fbi.gov

4. References:

- U.S. Coast Guard Maritime Industry Cybersecurity Resource Center: https://www.uscg.mil/MaritimeCyber/
- Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) - Port Facility Cybersecurity Risks: https://www.cisa.gov/sites/default/files/publications/port-facility-cybersecurity-risks-infographic_508.pdf
- National Security Agency (NSA), ODNI, and DHS/CISA - Developers Recommended Practices Guide for Securing the Software Supply Chain: https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF
- Federal Register - Entry on the Entity List (Nuctech): https://www.federalregister.gov/documents/2020/12/22/2020-28031/addition-of-entities-to-the-entity-list-revision-of-entry-on-the-entity-list-and-removal-of-entities
- Federal Bureau of Investigation (FBI) - Worldwide Threats to the Homeland: https://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland-111522
- H.R.7776 - James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Section: 3529): https://www.congress.gov/bill/117th-congress/house-bill/7776/text?q=%7B%22search%22%3A%5B%22National+Defense+Authorization+Act%22%2C%22National%22%2C%22Defense%22%2C%22Authorization%22%2C%22Act%22%5D%7D&r=22&s=3
- ODNI - 2023 Annual Threat Assessment of the U.S. Intelligence Community: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

5. Cancellation: This message cancels U.S. Maritime Advisory 2023-009 and will automatically expire on August 19, 2024.

For more information about U.S. Maritime Alerts and Advisories, including subscription details, please visit https://www.maritime.dot.gov/msci/ .