CISA publishes first Wärtsilä advisory after Cydome finds critical flaws in Wärtsilä's FOS software

The vulnerabilities could allow remote unauthorized users to deliver unauthorized updates to and execute code on the FOS system

LONDON, UNITED KINGDOM, September 28, 2026 /EINPresswire.com/ -- Cydome's maritime cyber research team has identified critical vulnerabilities in Wärtsilä FOS-Onboard version 5.07.0923.01. Wärtsilä's Fleet Optimisation Solution (FOS) is a voyage and fleet operations software. CISA published the advisory as ICSA-26-258-02 covering CVE-2026-78225 and CVE-2026-81855, rated as critical vulnerabilities (CVSS v4 scores of 9.5 and 9.3, respectively). Wärtsilä has confirmed to CISA that it has developed a security patch, available to its users.

> Despite the importance of the maritime industry to the global economy, cyber research in this field is scarce - especially regarding maritime-specific operational technology (OT)."
>
> *Alon Ayalon, VP R&D Cydome*

The vulnerabilities involve the use of a hard-coded cryptographic key in components of the FOS software, and their exploitation could allow a remote unauthorized user to deliver unauthorized updates to the FOS system, execute code, or extract credentials to allow the attacker to impersonate a privileged client.

The most direct consequence could be the ability of an attacker to gain a persistent trusted foothold in the FOS system, basically replacing it with a contaminated version without the operator's knowledge. This access allows attackers to manipulate operational data, gain access to other OT or IT systems connected to the FOS system, potentially risking operation of the vessel, compliance violation, and financial damage.

First Published Wärtsilä Vulnerability

Wärtsilä is a leading equipment and systems provider for the marine industry, claiming to have solutions installed on one in every three vessels sailing the oceans. Its marine business provides (among others): engines, propulsion and fuel supply equipment as well as marine navigation, fleet optimization and simulation solutions.

Despite its impact, very few people are looking at maritime OT

Having no published vulnerabilities is not unusual in this sector. While 90% of the world's goods travel by sea, maritime vessels operate highly specialized maritime systems, especially maritime operational technology (OT). Cybersecurity research as well as the compromise of marine OT requires a high level of expertise that few possess. While advanced generative AI tools lower the bar for cyber attackers and risks becoming more prominent (Cydome research found that the number of OT cyber incidents in 2025 showed a 150% increase), maritime OT cyber research remains largely a blind spot within the cybersecurity community, with very few published CVEs - including the CVEs published earlier this year by the Cydome research team.

"Despite the importance of the maritime industry to the global economy and the potential risk to shipping from cyber threats, cyber research in this field is scarce - especially regarding maritime-specific operational technology (OT). To help the industry become more resilient to the fast-evolving risks, Cydome conducts and publishes proactive research to identify threats and vulnerabilities before they disrupt operations."
Alon Ayalon, CTO and Co-Founder, Cydome

What operators should do now
Exploits of this vulnerability and similar severe vulnerabilities in maritime OT should be prevented by ensuring the following:
1. Operators should immediately update by deploying the latest patch that fixes the vulnerabilities.
2. Implement proper network segmentation that separates operational elements and OT from IT.
3. Ensure no unauthorized remote access is allowed.
4. Proactively run ongoing vulnerability scanning to prevent known critical vulnerabilities from being exploited.
5. Employ active cybersecurity monitoring using an intrusion detection system that can identify abnormal maritime OT network traffic to discover threats that manage to bypass other defenses or exploit a vulnerability that hasn't been published yet (Zero Day).

Cydome developed multi-layered cyber protection for maritime vessels rather than adapting office IT tools for the job.
"Maritime operations are transforming with hyper-connectivity through LEO technologies such as Starlink. But this digitalization, combined with the rapid adoption of AI, also expands the attack surface of critical OT assets. Cyber risk can no longer be managed reactively; organizations need continuous, active risk management embedded into their operational processes to protect vessels and the systems they depend on, and not rely on legacy solutions to protect their OT." said Ayalon. "Operators should not wait for a CVE to identify gaps in their cybersecurity; they should proactively deploy protection and continuously manage their cyber risks." he added.
Alon Ayalon, CTO and Co-Founder, Cydome

The flaw in the Wärtsilä software was discovered and shared in a responsible disclosure process

through CISA. It is the 9th CVE and the 3rd maritime product line Cydome's research team has published vulnerabilities in this year, following CVEs in Metis devices and NAVTOR NavBox.

Wärtsilä Response To The Findings
As part of the CISA advisory, Wärtsilä is quoted as stating that the vulnerabilities are not exploitable when the product is installed as recommended, and it has developed a security patch. Users are also directed to contact Wärtsilä to obtain and install the patch.

About Cydome
Cydome is a pioneer in research-led cybersecurity for maritime and critical infrastructure operations. Its products and managed services utilize Cydome's proactive cyber research and advanced AI technologies to provide fleet-wide monitoring, protection, threat prevention and integrated risk management for complex operations at sea. Trusted by leading maritime organizations and classification societies, Cydome protects vessels and offshore facilities around the world.

For additional maritime CVEs published by Cydome research, please see: https://cydome.io/cve

Shahar Dumai
Cydome
marketing@cydome.io
Visit us on social media:
LinkedIn
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/945634590

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.