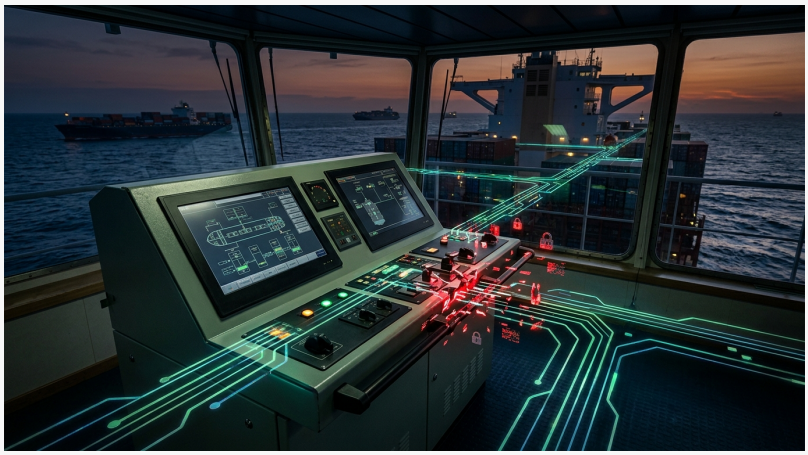
Cydome Research Identifies New Vulnerabilities in NAVTOR NavBox Devices That Could Expose Navigation and Network Data

Vulnerabilities published by Cydome could allow unauthenticated remote access to vessel telemetry and ECDIS data, amid 150% surge in maritime OT attacks.



New Vulnerabilities Expose Ship Navigation and Network Data

LONDON, UNITED KINGDOM, March 11, 2026 /EINPresswire.com/ -- Cydome, the leading provider of maritime-specific cybersecurity solutions, announced the discovery and responsible disclosure of three security vulnerabilities (CVEs) affecting the NAVTOR NavBox, a widely deployed operational technology (OT) gateway in the global shipping industry.

The vulnerabilities, identified in NavBox version 4.12.0.3, could allow unauthorized remote access to sensitive vessel telemetry, network configurations, and sensitive operational data such as ECDIS IP addresses. The vulnerabilities were shared with NavTor as part of Cydome's responsible reporting process, and NavTor acknowledged the findings, confirming they impacted NavBox v4.12.0.3 and have been remediated. NavTor also informed that affected customers were notified prior to the publication of the CVEs.

> Shipping companies are currently facing a significant gap. While their fleets become more connected with LEO broadband service, their OT devices are more exposed than ever to cyber threats."
>
> *Nir Ayalon, CEO of Cydome*

Fixed versions:
CVE-2026-2752: Fixed in version 4.16.2.4 (November 2025) and later.

CVE-2026-2753: Fixed in version 4.14.1.2 (December 2024) and later.

CVE-2026-2754: Fixed in version 4.16.2.4 (November 2025) and later. This discovery comes as Cydome's latest research reveals a 150% increase in cyberattacks targeting maritime OT over the past year. As shipping companies accelerate digitalization, once-isolated operational vessel systems are now connected to the internet, creating "blind spots" that traditional IT security tools often fail to see. In fact, the Cydome report shows that 50% of OT incidents begin with unauthorized external access, while cyber attackers use generative AI technologies to accelerate device exploitation even in areas that once required specialized expertise.

The Reality of OT Risks at Sea. For maritime IT managers overseeing global fleets, OT devices like the NavBox fulfill critical operational and safety functions. However, because of the highly specialized nature of those devices, which frequently employ unique maritime protocols, they are hard to patch or replace, and could be highly exposed to exploitation.

"Shipping companies are currently facing a significant gap," said Nir Ayalon, CEO of Cydome. "While their fleets become more connected with LEO broadband service, their OT devices are more exposed than ever to cyber threats. Cydome's mission is to promote the safety of the industry and sea travel, and as part of that, we identified and responsibly released the NavBox vulnerabilities to help shipping companies prevent the risk before it's exploited by malicious actors."

The Discovered Vulnerabilities The three vulnerabilities identified by Cydome's research team include:
CVE-2026-2752 – Missing Authentication on HTTP API Endpoints, CVSS V3: 7.5 HIGH, which could allow for unauthorized retrieval of network information.

CVE-2026-2753 – Absolute Path Traversal Vulnerability, CVSS V3: 7.5 HIGH, which could allow unauthorized retrieval of arbitrary files from the host operating system.
CVE-2026-2754 – Information Disclosure Vulnerability, CVSS V3: 5.3 MEDIUM, which could expose internal application details via stack traces.

A Collaborative Approach to Maritime Safety Cydome worked closely with NAVTOR to ensure a swift and responsible resolution of the vulnerabilities for all affected customers.
For more information on the research and technical advisories of the CVEs, visit:
https://cydome.io/cydome-discovered-three-vulnerabilities-in-navtor-navbox-version-4-12-0-3/

About Cydome: Cydome is a pioneer in maritime and critical infrastructure cybersecurity. Its multi-layer protection provides vessels, offshore facilities, and remote operational environments

with comprehensive IT and OT security, including network protection, automated vulnerability scanning, GPS spoofing detection, and centralized risk and compliance management, optimized for maritime and offshore assets and operational environments. Cydome is fully ISO/IEC 27001 and ISO/IEC 27017 certified, supporting evolving regulatory compliance requirements and serving shipping companies and offshore energy operators globally.

Shahar Dumai
Cydome
+44 330 808 3271
marketing@cydome.io
Visit us on social media:
LinkedIn
Facebook
YouTube
X
