U.S. COAST GUARD

MARITIME CYBER BULLETIN

18 November 2025

MCB 03-25: Proper Implementation of Multi-Factor Authentication

THREAT SUMMARY

Coast Guard Cyber Command (CGCYBER) has observed a notable increase in maritime cyber incidents directly attributed to the improper implementation of Multi-Factor Authentication (MFA). These incidents have often involved a threat actor using valid credentials, previously harvested through phishing campaigns or other means, to access accounts on Marine Transportation System (MTS) entities' networks.

MFA remains a proven and reliable safeguard against unauthorized access. However, CGCYBER has uncovered instances where MFA was either not enforced for certain users or was improperly configured. Given the increasingly sophisticated social engineering tactics being employed by malicious actors, strong and consistent application of access controls are critical.

Case Studies

In the third-quarter of 2025, CGCYBER's Maritime Cyber Readiness Branch (MCRB) observed three instances where a lack of MFA allowed threat actors to successfully gain initial access to victim's user accounts. In two of these instances, threat actors were able to gain access to employee email accounts and subsequently launch phishing campaigns against other employees and vendors because MFA was not enabled. In the third case, threat actors were able to compromise an account on a new laptop that did not have MFA properly configured in violation of company policy. In each of these incidents, proper MFA implementation would have likely safeguarded the MTS entities from these attacks.

Recommendations

CGCYBER advises maritime stakeholders to regularly review their access control policies. Maritime stakeholders should ensure all applicable employees have MFA correctly applied to their account or that compensating controls are implemented. IT personnel should review these policies with employees and follow standard procedures when connecting a new device to the company's network.

Resources

- CISA: Multi-Factor Authentication
- NIST: Multi-Factor Authentication
- NSA: Identity and Access Management

Resources

Facilities that observe any unusual or suspicious activity, breaches of security, or interruptions to their network should report those activities to:

Coast Guard's National Response Center:
1-800-424-8802

OR

Cybersecurity and Infrastructure Security Agency (CISA) Central:
1-888-282-0870

If you have any questions, please visit our website at:
https://www.uscg.mil/MaritimeCyber
or reach out to MCRB at:
maritimecyber@uscg.mil