U.S. Coast Guard and Federal Bureau of Investigation

Maritime Cyber Alert

Information Sharing Protocol: **TLP:CLEAR** (https://www.us-cert.gov/tlp)

September 4, 2026

Fortinet FortiGate Vulnerabilities

Summary

The United States Coast Guard Cyber Command and the Federal Bureau of Investigation (FBI) have observed a trend of nation-state threat actors exploiting vulnerabilities found in Fortinet FortiGate devices utilized by facilities and vessels in the Marine Transportation System (MTS).

The Cybersecurity and Infrastructure Security Agency (CISA) previously issued a report on this exploitation trend, also known as FortiBleed, across critical infrastructure and estimates that the credentials for 74,000 Fortinet devices, which include firewalls and virtual private network (VPN) gateways, have been compromised and leaked. In addition to brute force attacks and the use of compromised credentials for initial access, threat actors have been observed exploiting Common Vulnerabilities and Exposures (CVEs) to facilitate lateral movement, escalate privileges, and establish persistence.

Background

The Transportation Systems Sector remains highly attractive to adversaries seeking to disrupt supply chains and logistics. Threat actors routinely scan for specific, unpatched vulnerabilities to gain a foothold. Operators should aggressively prioritize remediation of internet-accessible vulnerable devices to prevent operational disruptions or lateral movement.

Mitigation Measures

CGCYBER recommends MTS partners implement the mitigations below which align with operational insights from CISA, FBI, and the Intelligence Community.

Patch known vulnerabilities

- Immediately identify and remediate the most prevalent targeted vulnerabilities for Fortinet devices (such as CVE-2026-24858 and CVE-2025-25252). FortiBleed itself has no associated CVE but it is important to minimize device attack surfaces.

Review Logs

- Retain and inspect logs in accordance with established industry standards, including firewall logs and VPN logs, for any irregular or unexpected activity.

Validate Network and Device Configuration

- Confirm segmentation of IT and OT, review firewall rules, and remain vigilant for unrecognized accounts. Consider modifying default ports to custom ports. Ensure proper version control and patch management on Fortinet devices.

Validate Credentials

- Reset potentially compromised credentials, especially at the administrative level, and follow strong password creation guidance, and ensure proper storage of credentials.

Enforce Strict MFA

- Require multi-factor authentication for all VPN user profiles and administrative portals.

End of Life devices

- Replace End of Life (EOL) devices no longer supported by the manufacturer, which present significant and frequently exploited security risks.

Resources

If your organization has any questions related to this alert, please contact the U.S. Coast Guard at: maritimecyber@uscg.mil, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at **202-372-2904**. To report a maritime cyber incident call the National Response Center 24x7 line at 1-800-424-8802.

- CISA Urges Hardening Fortinet Devices After Reports of Credential Exposure
- Analysis of Reported Credential Compromise of FortiGate Devices