United States Coast Guard

Maritime Cyber Bulletin

Bulletin 004-16 **January 5, 2016**

SHIPBOARD VOYAGE DATA RECORDER VULNERABILITIES

Overview

This Bulletin is provided to raise awareness in the maritime community of recent open source reporting highlighting cyber vulnerabilities associated with certain model(s) of Furuno Voyage Data Recorders (VDRs) and:

- Provide an overview of these vulnerabilities; and
- Provide mitigation and remediation information

Description

WHAT IS A VDR?

A VDR is an instrument installed on a ship to continuously record vital information related to the operation of a vessel akin to the "black box" found on aircraft. VDRs enable accident investigators to review procedures and instructions in the moments before an incident and help to identify the cause of any accident. A VDR typically records:

- Date and Time
- Ship's Position
- Speed and Heading

- Bridge and Communications Audio (radio)
- Radar Data
- Electronic Chart Display and Information System (ECDIS) Information (if equipped)
- Wind Speed and Direction
- Echo Sounder/Fathometer Data
- Main Alarms
- Rudder Order and Response
- Hull Opening Status
- Watertight and Fire Door Status
- Automatic Identification System (AIS) Data

Details on carriage requirements and performance standards for VDRs can be found here.

Vulnerability Detail

Researchers at IOActive documented numerous vulnerabilities when examining the Furuno VR-3000 VDR. The researchers reportedly found; buffer overflows, command injection vulnerabilities, weak encryption and a flawed firmware update mechanism.

A copy of the full IOActive report can be found here.

Technical Details

According to technical analysis conducted by CERT/CC, the Furuno VDR models VR-3000, VR-3000S and VR-7000 moduleserv firmware update utility fails to properly sanitize user-provided input and is vulnerable to arbitrary command execution with root privileges. The impact of this vulnerability could allow an unauthenticated attacker with network access to affected devices to execute arbitrary commands with root privileges allowing for the manipulation of data captured on the VDR.

A copy of the CERT/CC technical analysis can be found here.

Risk Mitigation

To address these vulnerabilities, Furuno released several software updates. Recommended updates should be applied as follows:

- For VR-3000 and VR-3000S models:
  - V1.50 through V1.54 should be updated to V1.56
  - V1.61 should be updated to V1.62
  - V2.06 through V2.54 should be updated to V2.56
  - V2.60 through V2.61 should be updated to V2.62

- For VR-7000 models:
    - V1.02 should be updated to V1.04

A copy of the Furuno release discussing these software updates can be found here.

References

- Carnegie Mellon University CERT Vulnerability Note VU#820196
- Furuno Voyage Data Recorder Web Page
- IOActive Blog Voyage Data Recorder
- Maritime Safety Committee Resolution MSC.333(90)
- International Maritime Organization

Questions

For maritime cyber safety and security questions or questions related to this report, contact the U.S. Coast Guard Liaison Officer to the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) at:

Email: CGNCCICLNO@hq.dhs.gov

Phone: (703) 235-8850

Feedback

Your feedback is important to us. Please e-mail any comments and/or feedback on this product to CGNCCICLNO@hq.dhs.gov.