NMFTA
National Motor Freight
Traffic Association, Inc.

Heavy Vehicle Cyber Security Update

National Motor Freight Traffic
Association, Inc.
1001 North Fairfax Street, Suite 600
Alexandria, VA 22314
(703) 838-1810

Electronic Logging Device (ELD) Cybersecurity Bulletin

Bulletin Name	Issue Date	Last Updated	Version
Electronic Logging Device (ELD) Cybersecurity Bulletin	August 28, 2017	May 30, 2018	1.1

As most people in the industry are aware, the FMCSA's ELD mandate becomes mandatory for most carriers as of December 18, 2017. In general, NMFTA does not take an adverse position on the ELD mandate itself but NMFTA has identified some concerns regarding the implementation of the ELD mandate.

Contrary to some reporting in news media, as far as NMFTA has been able ascertain the current ELD rule, as written and implemented, requires both two way CAN bus connectivity and internet connectivity. This creates some genuine concern regarding the cyber security posture of the ELD devices themselves as they create a bridge between the internet and the CAN bus network of the vehicle. If the ELD devices could be exploited to send malicious traffic to the vehicle CAN bus, it could have serious consequences to the safe operation of the vehicle. While existing and proven device manufacturers hold the majority of the ELD market, the new mandate has brought a number of new entrants into the market hoping to capitalize on the opportunity. NMFTA's concerns focus mostly on these entry level device manufacturers whose solutions at times are to simply connect a consumer cell phone directly to the J1939 diagnostic port or to use a very basic hardware solution with built-in cellular capabilities.

At Blackhat USA 2017 and DEF CON 25, IOActive released a summary of their findings while analyzing three entry-level Electronic Logging Device (ELD) providers that were listed as self-certified from the Federal Motor Carrier Safety Administration (FMCSA) website. Their general conclusion was that all three devices did very little to nothing at all to follow cybersecurity best practices and were open to compromise. They noted the following specific shortcomings in their report:

- Devices shipped with debug enabled
- Firmware easily accessible for analysis
    - Development strings present
    - Use of banned functions
- Lack of secure boot
- Lack of encryption for communications
- Basically a general failure to follow cybersecurity best practices

It was also noted by IOActive that the FMCSA ELD Test Plan and Procedures document contains "Insert the Quality Assurance program here." in the content of section "1.11 Quality Assurance". This document is described by FMCSA as "FMCSA provided these specifications to confirm compliance of an ELD with independent testing and validation".

NMFTA has been unable to find any recommendations or guidance for cyber security for the actual ELD devices in this document with the exception of sections 4.10.1.1 and 4.10.1.3 which refer to encryption when communicating with FMCSA servers or sending data via email. No specific requirements for device cyber security were discovered during our investigation.

We would therefore strongly recommend that, before you deploy any type of ELD device, you contact the manufacturer/supplier of the device and obtain specific and detailed information regarding the cyber security posture of the device. Specifically, ask about the technical standards or best practices followed (if any) as well as if adversarial testing or 3rd party security evaluations were performed as part of their product development lifecycle. Awareness of the issue is a critical first step in protecting your fleet and/or equipment.

Given the security/quality issues described by IOActive in their report, NMFTA also feels that there is a risk that malfunctioning or poorly designed and implemented ELD devices could create an increase in vehicle maintenance issues due to faulty or erroneous CAN network data transmissions. The types of issues that could arise could be difficult to diagnose and reproduce and maintenance departments and OEMs should prepare themselves as need to handle the potential for these types of problems.

NMFTA will continue to monitor the cyber security issues surrounding the ELD mandate and work to identify risks and as much as possible work with industry and government to mitigate and reduce the risks.