Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 July 2020

PIN Number
20200721-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

Electronic Logging Device Cybersecurity and Best Practices

Summary

Cyber criminals could exploit vulnerabilities in electronic logging devices (ELDs), which became required equipment in most commercial trucking operations as of 16 December 2019 due to a federal regulatory mandate. Although the mandate seeks to provide safety and efficiency benefits, it does not contain cybersecurity requirements for manufacturers or suppliers of ELDs, and there is no requirement for third-party validation or testing prior to the ELD self-certification process. This poses a risk to businesses because ELDs create a bridge between previously unconnected systems critical to trucking operations. Companies choosing an ELD can mitigate their cyber risk by following best practices tailored to ELDs. This includes asking the ELD's supplier specific questions, some of which are identified in this PIN.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

ELD Connectivity and Security

ELDs are devices that electronically send inspection reports to the Federal Motor Carrier Safety Administration (FMCSA). ELDs are required to connect to a vehicle's electronic control module (ECM) in order to track date, time, location information, engine hours, vehicle miles, user identification data, vehicle identification data, and motor carrier identification data. ELDs must also permit wireless connectivity. As a result, ELDs create a bridge between critical vehicle components and wireless data transmission, such that the vehicle components themselves can be accessed remotely through Wi-Fi or Bluetooth. The most common implementations of ELDs use built-in cellular modules, but satellite, Bluetooth, or cabled tethering to cellular enabled smart phones and tablets are also options.

The ELD mandate does not contain any cybersecurity or quality assurance requirements for suppliers of ELDs. As a result, no third-party validation or testing is required before vendors can self-certify their ELDs. Businesses choosing an ELD to use on their networks must therefore conduct due diligence themselves to mitigate their cyber risk and potential costs in the event of a cyber incident.

The Department of Transportation (DOT) FMCSA ELD mandate entered the third and final phase on 16 December 2019, requiring the use of self-certified ELDs registered with FMSCA by all drivers and carriers subject to the rule.

ELDs and Cyber Threats

Industry and academic research into a selection of self-certified ELDs found the sample of devices did little to nothing to follow cybersecurity best practices and were vulnerable to compromise. The sample included ELDs that could be purchased off the shelf at superstores and ELDs supplied by well-known companies. Researchers demonstrated the potential for malicious activity to remotely compromise the ELDs and send instructions to vehicle components to cause the vehicle to behave in unexpected and unwanted ways. Although the ELDs are only intended to allow the logging of data from the engine, in practice some self-certified ELDs allow commands to be sent to the truck engine via their connection to the ECM. Commands passed into the vehicle network through an ELD could affect functions such as vehicle controls and the accuracy of the console display. Potential indicators of this occurring include an increase in nonreproducible equipment performance or maintenance issues, an increase in traffic on the vehicle's internal network, or networking logs for the ELD showing

unexpected incoming remote connections. The limited indicators and warning signs for this type of activity increase the importance of selecting a secure device with settings that restrict traffic during normal operations.

ELDs with more advanced telematics functions and a connection to functions such as shipment tracking or dispatching can allow a cyber actor who gains access to an insecure ELD to move laterally into the larger company business network. Cyber criminals interested in stealing data such as personal information, business and financial records, location history and vehicle tracking, or other proprietary data such as lists of customers and cargo can use vulnerabilities in ELDs as a way in to access trucking companies' enterprise networks and databases. With that access, financially motivated cyber criminals would also be positioned to install malware such as ransomware, preventing the ELD, the vehicle, or connected telematics services such as dispatching or shipment tracking from operating until the ransom is paid. Potential indicators for this kind of malicious activity include unusual traffic or unusual file sharing on the network, which could best be detected by establishing a network baseline and monitoring network loads and traffic, as well as restricting user and device access privileges to only what is needed for their job.

How to Mitigate the Risk: Questions to Ask ELD Makers and Suppliers

Before deploying an ELD, it is recommended to contact the manufacturer or supplier of the ELD and ask about its cybersecurity. When contacting suppliers, seek specific and detailed information regarding the security of the entire ELD solution. Because ELDs can include a combination of in-vehicle, communications link, user interface, and cloud back-end systems, the supplier should be asked for details that address the cybersecurity of all functions and components.

In May 2020, DOT FMCSA released a set of cybersecurity best practices for ELD solutions in "*Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems*" [FMCSA-RRT-19-013]. The best practices provide guidance regarding considerations for trucking companies when acquiring new devices and what suppliers can expect from customer acceptance testing of these requirements.

DOT-FMCSA's best practices cite a 2018 report by the National Motor Freight Traffic Association (NMFTA). NMFTA recently released an updated 2020 document on the same topic: *"NMFTA Cybersecurity Requirements for Telematics Systems."* The cybersecurity guidance in Appendix A

of the updated NMFTA document includes a rating for cybersecurity considerations, ranking them as low, medium, or high criticality. The document recommends that solutions failing to satisfy high-criticality requirements should be avoided, but solutions failing to satisfy medium-criticality requirements may still be considered for purchase with justification by the supplier, and low- criticality requirements may still be considered even without justification by the supplier. For example:

- *Is the communication between the engine and the ELD enforced?* [SCP-060] is a high-criticality requirement, and the report recommends that any ELD to be purchased must satisfy this requirement.
- *Were technical standards or best practices followed in the device's development?* [SII-150] is a medium-criticality requirement, and solutions not satisfying this can still be acceptable for purchase with supplier justification.

Other requirements of note include:

- *Does the component protect confidentiality and integrity of communications?* [requirement SCP-010] This applies to each component of an ELD solution.
- *Has the component had penetration tests performed on it?* [SAA-020] Also applies to each component or possibly the system as a whole; however, asking the question for each component makes supplier responses clear.
- *Does the device have secure boot?* [SII-040] Applies to any device that could be in attacker hands; in some ELD solutions, this will be all of the vehicle-connected devices, a modem, and a smartphone, as indicated in the report.
- *Does the device ship with debug mode enabled?* [CM-030] Applies similarly to all devices, which may be one, two, or three devices for the solution, as indicated in the report.

Insecure devices, even if not specifically targeted by cyber criminals, can experience issues in stability or performance resulting from interference or opportunistic infection. An active approach to vetting ELD options before implementation is a small up-front investment of time that mitigates the risk of costly or disruptive cyber incidents in the long run.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey