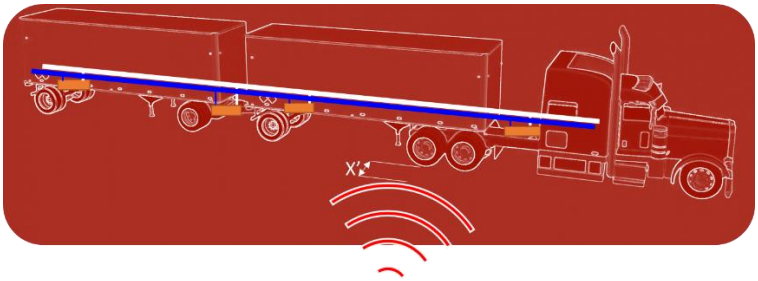
March 3, 2022

To whom it may concern,

NMFTA is a nonprofit membership organization comprised of approximately 500 motor freight carriers operating in interstate, intrastate and foreign commerce primarily specializing in the movement of less-than-truckload (LTL) quantities of freight. NMFTA's mission is to promote, advance and improve the welfare and interests of its members and the motor carrier industry in general. In 2015, we initiated a program to study the cyber security vulnerabilities of heavy vehicles. For the past 3 years, among other projects, we worked together with Assured Information Security, Inc. (AIS) to investigate cyber security weaknesses in trailer Power Line Communications (PLC): J2497 aka PLC4TRUCKS. In the interest of responsible disclosure, we are writing to you to share a follow-up confirmation of results from our investigation previously disclosed in November 2019.



Our research indicates that J2497 (PLC4TRUCKS) receivers are susceptible to remote RF induced signals. This can be accomplished with a range of equipment costs for a range of distances from ~300 USD to ~10KUSD and up to 12ft. We have found that all 3 trailer ABS supplier's equipment are affected. Additionally, both tractor ABS controller supplier's equipment are also affected. We have found that some trailer configurations/types are more susceptible to RF induced J2497:

- tankers
- 3x 'pup' road trains, any decking

Because testing has been limited to what equipment was available to us, we also have the following very likely but also still theoretically-only susceptible targets:

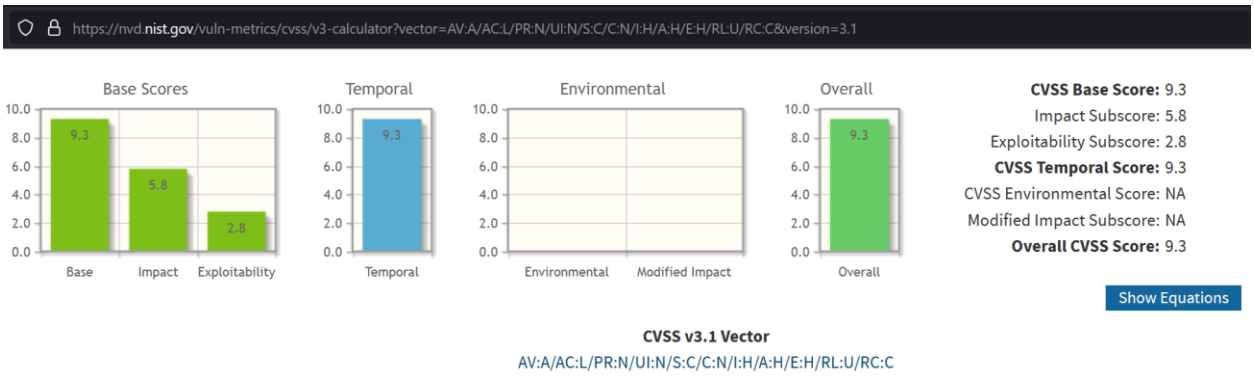
- 2x 'pup' road trains with extruded metal decking – because a single pup with metal extruded decking was only a little less susceptible than a 3x pup road train with wood decking
- flat beds (including intermodal trailers) – because their wiring runs outside along a metal structure as with tankers
- 2x 40' road trains, any decking – because the total length is equivalent to a 3x pup road train

Even though the above are theoretical-only our current understanding of the technology and the attack (which correctly predicted tankers and 3x road trains) leads to the conclusion that they would be susceptible as well.

1001 North Fairfax Street, Suite 600 ♦ Alexandria, VA 22314-1798 ♦ ph: 703.838.1810 ♦ fax: 703.683.6296

web: www.nmfta.org ♦ email: nmfta@nmfta.org

We estimate this vulnerabilities' overall CVSS (v3) score at 9.3, with vector AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:H/E:H/RL:U/RC:C. Most notably this vulnerability has a proven exploit and yields scope change in addition to compromising availability and integrity. This score does not account for the potential tractor-trailer availability and safety impacts.

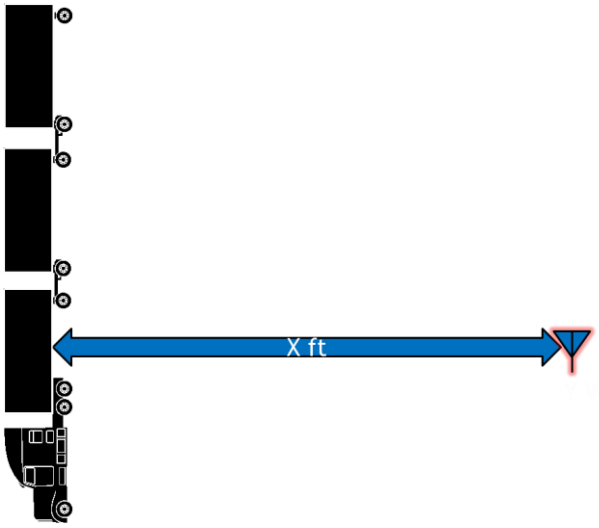


[REDACTED to https://ctsrp.nmfta.org]

We have achieved successful induced J2497 on the following 3 trailer configurations/types. The results were confirmed on all 3 trailer ABS supplier's equipment by swapping the trailer ABS unless otherwise noted:

- 20 ft dry-van 'pup' built with extruded metal decking
- 50 ft tanker trailer
- Triple (3x trailers and 2x dollies) 20 ft dry-van 'pup' with wooden decking (confirmed on the single trailer OEM's ABS supplier)

The testing method for all of the above followed the same process:



1. Transmit a J2497 signal on a loop which encodes all 3x trailer ABS solenoid tests on all 5x possible dynamic addresses plus a tractor ABS 'roll-call' command.
2. For each varied distance of the antenna from the trailer (driver's side):
3. Increase the transmit power until solenoid clicks and/or air chuffs are observed

Induced J2497 on Dry Van 'pup' w. Extruded Metal Decking (confirmed on all 3x Trailer-ABS):

Distance, Driver-side [ft]	Minimum Power [W]
1.5	12.5
3	Unknown (but >50)

Induced J2497 on 50' Tanker (confirmed on all 3x Trailer-ABS):

Distance, Driver-side [ft]	Minimum Power [W]
3	1.5
5	2
8	10
11.5	12.5
22	Unknown (but >45)

Induced J2497 on a 'Triple' w. Wood Decking and Steel Framing:

Distance, Driver-side [ft]	Minimum Power [W]
1.5	40
3	40
4.5	75

6	100
8	160
20	Unknown (>160)

Some important observations from the results achieved:

- The attack works on all trailer ABS supplier's equipment and appears to be possible with any J2497 receiver (e.g. Intellon SSC P485) connected to susceptible equipment
- Tanker trailers are very susceptible. We suspect this is also true of flatbeds but have not had a testing opportunity
- Some dry-vans are more susceptible than others. It appears that those with extruded metal decking are the most susceptible
- Road trains make the equipment more susceptible. e.g. a single pup with wood decking was not susceptible from 1.5ft @ 100W transmit power but was susceptible from 6ft @ 100W in a triple configuration

This remote J2497 write vulnerability matters because an attacker is able to directly reach both the trailer and tractor brake controllers. All trailer ABS equipment from all suppliers listens and reacts to commands on J2497 without authorization and authentication and our research indicates that tractor brakes controllers do so also -- including when configured not to perform J2497 gateway functionality. In our testing, we have proven solenoid test, 'roll-call', and LAMP ON (as required to perform the only industry standard way to satisfy FMVSS 121 paragraph S5.1.6.2(b)) commands. There is also the possibility of more effective commands for dumping air supply and/or vulnerabilities in the trailer and tractor brake controller's firmware which could yield this result or worse. Trailer brake suppliers are in the best position to assess the likelihood of these worse-impact attack vectors; we have not performed reverse engineering of tractor nor trailer brake controller firmware to assess this.

However, solenoid test alone is sufficient to bleed supply air in the case where the brake control pressure signal is applied. Or even without a brake control signal applied in the case of dollies. As such, our current understanding of the functionality available to the attacker enables practical attacks of concern to the fleets and to the industry:

- Practical distance for well-funded attackers is good enough to put transmitters at choke points on the roadway infrastructure (e.g. ports, rail crossings, tunnels, bridges, etc.)
- It is also possible to stage mobile transmitters in long trailers (garden or car transport) towed by passenger cars
- For the most susceptible equipment, tankers: an attack on a tight budget can succeed at distances of a lane separation or even ditch-to-road.
- It is also possible to light the trailer ABS fault lamp in the cab, thereby influencing the driver to pull-over. But this almost certainly a stop at a safe location unlike the above impactful attacks.

In summary, trailer and tractor brake ECUs have a great deal of J2497 functionality beyond the required LAMP messages. We have made a signal which will 'chuff' all trailer brake supplier's controllers at all dynamic addresses and 1 of 2 tractor brake controllers (so far) – on a loop without any authorization or authentication obstructing the success of the signal. Induced J2497 RF transmission of this PoC signal (and of any other signal an attacker could concoct) is practical and sometimes even cheap. This attack yields attacks of concern to fleets and the industry. The attacker equipment involves an SDR, signal conditioning, linear power amplification and a 9:1 balun driving a wire antenna. Power amplification costs vary but the remaining equipment is not expensive, nor is it particularly novel or difficult to install.

Please note that we do not believe that we are the only people to have considered this attack in the 20 years that J2497/PLC4TRUCKS has been fielded. Anecdotally, whenever we have presented our work on remote read (e.g., ICSA-20-219-01) an audience member has asked about remote write and more than a couple times has described how it could be possibly be achieved.

We believe that in the long term, tractor-trailer interfaces should permit only the required LAMP messages from trailers to tractor and nothing else. No diagnostics, resets, or other data link escape commands over J2497 on either tractor or trailer equipment. This requirement was included in the draft RP1217 sent to ballot in September 2021 at ATA TMC Fall meeting.

The industry is approaching a transition to other tractor-trailer interconnects and J2497 will be needed only for backwards compatibility. It is possible in this transition for tractor equipment to accept at J2497 ingress only the LAMP ON message and for the trailer equipment to drop all frames on ingress and only send LAMP ON to communicate fault conditions. Even so this will still enable RF induced LAMP ON messages which could influence a driver to pull over; we aren't aware of a way to maintain backwards compatibility and avoid this particular attack.

In the short term, something needs to be done to mitigate the risk to at least the most susceptible equipment. We have been researching and developing mitigations during our time investigating this issue. We have captured the extent of our knowledge of protections to J2497 attacks in the document, *Actionable Mitigations Options for J2497 Attacks*; where we have also collected some solutions concepts which we believe have merit in reducing the risk for the fleets. We are also open to collaboration on the development and qualification of unencumbered mitigations for the fleets.

The goal of the disclosure is to mitigate the risks to the fleets as soon as possible. To that end and because the preliminary results of this investigation have already been shared in November 2019, we have already disclosed this information to the U.S. FBI Cyber Division and to U.S. DHS CISA. We intend to notify the Auto-ISAC by sharing a copy of this letter in four business days, on January 21 2022. Sharing the information wider will continue at a pace selected in collaboration with CISA, ultimately aiming to reach also trailer OEMs and fleets. To achieve the goal of mitigating the fleet risks as soon as possible, we intend on sharing the *Actionable Mitigation Options for J2497 Attacks* with them as part of the disclosure process. We especially need to reach fleets with large numbers of tankers and road trains.

We are available to you and your technical experts to discuss the results of our research. Please contact me at your earliest convenience. We will aim to include our research partners, Assured Information Security (AIS), in discussions whenever possible.

Best Regards,

Ben Gardiner

Senior Cybersecurity Research Engineer
National Motor Freight Traffic Association, Inc.
1001 N. Fairfax St., Suite 600
Alexandria, VA 22314

E-mail: ben.gardiner@nmfta.org
Phone: +1 (703) 838-1825
Fax: +1 (703) 683-6296
www.nmfta.org