/ Case Study / Rail / Penetration Test

How a series of 'low risk' vulnerabilities led to a global compromise of services across 3000 trains

Introduction

Penetration tests of industrial and operational technology (OT) platforms often uncover the same insecure configurations, unsupported legacy systems and poor password management. These OT environments have often been operational in a vulnerable state for long periods, often only protected by a lack of connectivity and discoverability.

As new equipment is added to supply passenger entertainment, monitoring and onboard data analytics, systems and associated networks are required to be more connected. Nonetheless, traditional safety concerns (electrical, etc) and productivity requirements remain the primary goals.

Here's how a well scoped penetration test helped identify unknown risks to a UK train operator, the Department for Transport and rail operators around the world.

During the opening scoping meetings with the Train Operator, manufacturers and digital equipment vendors, it became clear that the threat models initially applied within the rail industry have historically been based on business and safety risks experienced to date, such as vandalism, passenger or staff error, and events leading to service disruption such as hoax calls. The majority of these 'traditional' threats could probably only be enacted on small scales, for example, by targeting a single train or station and potentially with the impact of causing temporary disruption. We were keen to identify attack paths that accounted for the end goals of the adversaries targeting UK CNI.

This meant adding onboard systems and networks into the scope of the security assessment, as well as Internet connected systems including data, monitoring and shared services provided by third-parties.

ABOUT MODUX

Founded in 2008, Modux provides combined cyber security and technology research services into Critical National Infrastructure, FTSE100s & UK Government

modux

The first part of the engagement involved a deep-dive assessment of technical documentation, network architecture and engineering manuals. This provided the team with enough understanding of what attacks might be possible, but also demonstrated the potential impact of successful exploitation.

Following this, the technology was reviewed in a lab setting, which consisted of penetration testing against a representative test-bench as well as reverse engineering of network equipment that could be obtained commercially. This allowed the team to construct a test plan which helped ensure that onboard testing wouldn't be disruptive to live rail operations.

Penetration testing was then performed across a number of different train units, based around the availability and service schedule of the TOC. Full assessments of the media and engineering networks were performed, as well as realistic assessments using the passenger Wi-Fi and accessible switch cabinets to assess what activities a malicious passenger may be able to perform during a journey.

With the combination of technical assessments and penetration testing activities from different points on the network, the team were able to understand what attacks would be possible by an uninformed threat actor with the gift of time on their side.

By leveraging shared services used for onboard monitoring, it was possible to gain control of critical onboard and wayside systems across the rail fleet. Furthermore, the access gained during these testing activities allowed full remote access onto trains across operators across Europe and the Americas. These operators are not commercially related, but subscription to shared services had led to a vast number of trains being interconnected, unbeknownst to the operators, ROSCOs or manufacturers.

Observed and compromised systems included OT, but not limited to Driver Advisory Systems (DAS), Train Control Management Systems (TCMS), CCTV & NVR, as well as Automatic Selective Door Operating system (ASDO) and interconnected braking systems.

For those in rail, the impact of such results may be obvious. Information based systems such as the DAS could be manipulated to modify headcodes and train speed readouts. Moreover, OT could have been leveraged to perform safety critical mechanical operations based around unauthorised access, replay attacks and modified data inputs.

Furthermore, Modux identified multiple previously unknown remote code execution vulnerabilities in onboard systems including Moxa switches.

Outcomes

These findings were presented directly to the Department for Transport, NCSC, third-party service providers as well as representatives of various train operators.

Remediation work and advice was performed in partnership with the Train Operator and service providers to implement stricter security controls resulting in more secure onfleet systems, enhanced attack monitoring as well as stricter policies for the management of these systems.

The remote code execution and privilege escalation vulnerabilities were reported to the vendors. The Modux research team worked with these to advise on vulnerability exploitation and remediation.