Kaspersky Lab helps uncover vulnerabilities that make petrol stations easy prey for hackers

7 February 2018

Kaspersky Lab researchers have helped uncover a number of unknown vulnerabilities that have left petrol stations around the world exposed to remote takeover, often for years. The vulnerabilities were found in an embedded petrol station controller of which there are currently over 1,000 installed and online. The manufacturer was notified when the threat was confirmed.

Ido Naor, senior security researcher at Kaspersky Lab, together with another researcher found the controller during unrelated research into devices with open connections to the internet. In many cases the controller had been placed in the fuel station over a decade ago and had been connected to the internet ever since.

The controller, which runs a Linux machine, operates with high privileges and the researchers discovered a number of vulnerabilities that leave the device and the systems it is connected to open to cyberattack. For example, the researchers were able to monitor and configure many of the petrol station settings. An intruder able to bypass the login screen and gain access to the main interfaces would be able to do any of the following:

- Shut down all fueling systems
- Change the fuel prices
- Cause fuel leakages
- Circumvent payment terminals to steal money (the controller connects directly to the payment terminal, so payment transactions could be hijacked)
- Scrape vehicle license plates and driver identities
- Execute code on the controller unit
- Move freely within the petrol station network

"When it comes to connected devices it is easy to focus on the new and to forget about products installed many years ago that might be leaving the business wide open to attack. The damage that could be done by sabotaging a petrol station doesn't bear thinking about. We have shared our findings with the manufacturer," said Ido Naor, Senior Security Researcher at Kaspersky Lab.

The vulnerabilities have also been reported to MITRE and the research is ongoing.

Kaspersky Lab advises manufacturers of connected internet-of-thing devices to consider the security of their products from the very first moment of development and design, and to review legacy devices for possible security vulnerabilities. Users of connected devices are urged to review regularly the security of these devices and not to rely on factory settings.

More information on the research is available on Securelist.

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company that celebrated its 20 year anniversary in 2017. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialised security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at https://www.kaspersky.co.uk/.

Editorial contact:

Berkeley Global
Ollie Bennett
kasperskylab@berkeley.global
Telephone: 0118 909 0909
100 Longwater Avenue

Kaspersky Lab UK
Stephanie Fergusson
Stephanie.Fergusson@kasperskylab.co.uk
Telephone: 07714107292
2 Kingdom Street