Trend Micro Research Uncovers Security Risks Facing Connected Industrial Machinery

Radio frequency remote controller weaknesses have serious safety implications

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released a new report detailing inherent flaws and new vulnerabilities in radio frequency (RF) remote controllers found and disclosed through the Zero Day Initiative (ZDI). The report, *A Security Analysis of Radio Remote Controllers for Industrial Applications,* demonstrates how an attacker could persistently and remotely take control of, or simulate the malfunction of, the attacked machinery.

The report's findings cover RF remote controllers found in cranes, drills, mining machinery and other industrial devices produced by the seven most commonly deployed vendors. These types of devices have become a major point of security weakness because of their connectivity. Long lifespans, high replacement costs, and cumbersome patching processes compound this problem.

"This research demonstrates a concerning reality for owners and operators of heavy industrial machinery where RF controllers are widely found," said Bill Malik, VP of infrastructure strategies for Trend Micro. "By testing the vulnerabilities our researchers discovered, we confirmed the ability to move full-sized industrial equipment deployed at construction sites, factories, and transportation businesses. This is a classic example of both the new security risks that are emerging, as well as how old attacks are being revitalized, to attack the convergence of OT and IT."

Trend Micro discovered three basic failings in RF controllers: no rolling code; weak or no cryptography; and a lack of software protection. Leveraging these basic weaknesses enabled five remote and local attack types, which are detailed in the report. To help facilitate the research, an RF analyzing tool, RFQuack, was also developed.

Many operational technologies in industrial settings are now facing cyber risks due to newly added connectivity. According to Gartner, "IoT devices must remain secure for many years, potentially decades. IoT devices are also exposed or unprotected. This combination of time and space presents a different security profile than that of traditional IT assets. Security and risk management leaders must identify key industrial assets and systems, and prioritize protection of these assets based upon their mission criticality and integrated risks to OT and IT systems."1

Beyond prioritizing the cyber risks associated with these devices, Trend Micro recommends companies that use RF controllers implement comprehensive security measures, including software and firmware patching, as well as building on standardized protocols.

To read the complete Trend Micro research report, please visit: https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud workloads, networks, and endpoints. With more than 6,000 employees in 50 countries and the world's most advanced global threat research and intelligence, Trend Micro enables

organizations to secure their connected world. For more information, visit www.trendmicro.com.

1 Gartner, *Cool Vendors in Industrial IoT and OT Security*, *2018*, Saniye Burcu Alaybeyi, Wam Voster, Prateek Bhajanka, James McGovern, Barika L Pace, 26 April 2018

Contact:

Erin Johnson
817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.ca/2019-01-15-Trend-Micro-Research-Uncovers-Security-Risks-Facing-Connected-Industrial-Machinery