Trend Micro Research Uncovers Major Flaws in Leading IoT Protocols

Hundreds of thousands of unsecured machine-to-machine deployments put global organizations at risk

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today warned organizations to revisit their operational technology (OT) security after finding major design flaws and vulnerable implementations related to two popular machine-to-machine (M2M) protocols, Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP). Trend Micro's new report, co-branded with Politecnico di Milano, *The Fragility of Industrial IoT's Data Backbone,* highlights the growing threat of industrial espionage, denial-of-service and targeted attacks by abusing these protocols.

Over just a four-month period, Trend Micro researchers identified more than 200 million MQTT messages and more than 19 million CoAP messages being leaked by exposed brokers and servers. Using simple keyword searches, malicious attackers could locate this leaked production data, identifying lucrative information on assets, personnel and technology that can be abused for targeted attacks.

"The issues we've uncovered in two of the most pervasive messaging protocols used by IoT devices today should be cause for organizations to take a serious, holistic look at the security of their OT environments," said Greg Young, vice president of cybersecurity for Trend Micro. "These protocols weren't designed with security in mind, but are found in an increasingly wide range of mission critical environments and use cases. This represents a major cybersecurity risk. Hackers with even modest resources could exploit these design flaws and vulnerabilities to conduct reconnaissance, lateral movement, covert data theft and denial-of-service attacks."

The research shows how attackers could remotely control IoT endpoints or deny service by leveraging security issues in the design, implementation and deployment of devices using these protocols. Furthermore, by abusing specific functionality in the protocols, hackers could maintain persistent access to a target to move laterally across a network.

A few vulnerabilities were also identified through this research, which were disclosed through Trend Micro'sZero Day Initiative (ZDI): CVE-2017-7653, CVE-2018-11615, and CVE-2018-17614. An example of the impact these vulnerabilities could have, CVE-2018-17614 is an out-of-bounds write that could allow an attacker to execute arbitrary code on vulnerable devices that implement an MQTT client. While no new CoAP vulnerabilities were found, the report reinforces that CoAP is User Datagram Protocol-based and follows a request-response scheme, making it a good fit for amplification attacks.

To mitigate the risks highlighted in the research, Trend Micro encourages organizations to:

- Implement proper policies to remove unnecessary M2M services
- Run periodic checks using internet-wide scanning services to ensure sensitive data is not leaking through public IoT services
- Implement a vulnerability management workflow or other means to secure the supply chain
- Stay up to date with industry standards as this technology is evolving rapidly

To read the complete report, please visit:https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mqtt-and-coap-security-and-privacy-issues-in-iot-and-iiot-communication-protocols.

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. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection. 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.

Contact:

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

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.com/2018-12-04-Trend-Micro-Research-Uncovers-Major-Flaws-in-Leading-IoT-Protocols