Kaspersky Lab helps to eliminate seven vulnerabilities in Industrial IoT Platform solution

Kaspersky Lab experts have helped to identify and patch seven previously unknown vulnerabilities in the ThingsPro Suite – an industrial IoT platform, designed for industrial control systems (ICS) data acquisition and remote analysis. Some of the vulnerabilities found could potentially allow threat actors to gain highly priviledged access to industrial IoT gateways and execute deadly commands. All vulnerabilities identified were reported to and patched by platform developer Moxa.

ThingsPro Suite is an industrial internet of things platform that automatically gathers data from Operational Technology (OT) devices running at the industrial facility and submits it to an IoT cloud for further analysis. However, as much as such platforms are useful to ease IIoT integration and maintenance, they can also be dangerous, unless they are developed and integrated with adequate security concerns in mind. As such solutions work as a connecting point between IT and OT security domains, vulnerabilities found in them can potentially allow attackers to gain access to an industrial network.

Within two weeks, Kaspersky Lab ICS CERT security researchers have been conducting a preconceptual study of the product, testing it for vulnerabilities that could be exploited remotely. As a result, seven zero-day vulnerabilities were found. One of the most severe could allow a remote attacker to execute any command on the target IIoT gateway. Another vulnerability made it possible for cybercriminals to gain root privileges, providing the ability to change the device's configuration. Moreover, its exploitation could be automated, meaning that cybercriminals could automatically compromise multiple Moxa ThingsPro IoT gateways in different enterprises and to even potentially gain access to industrial networks of the organizations.

"Moxa is a trusted and respected brand in the industrial systems world. However, despite the company's vast expertise and experience, its new product had a number of vulnerabilities, which shows that it is important even for industry leaders to conduct proper cybersecurity tests. We call on all ICS-product developers to act responsibly, performing regular vulnerability checks, treating the security of solutions for industrial systems as an integral and essential part of development," said Alexander Nochvay, security researcher at Kaspersky Lab.

To keep industrial control systems safe, we advise that companies:

• Restrict access of IIoT gateway devices to components of the enterprise's OT and IT networks to the extent possible;

• Restrict access to IIoT gateway devices from the enterprise network and the internet to the extent possible;

• Set up monitoring of remote access to the enterprise's OT network, as well as monitoring of access to individual ICS components (workstations, servers, and other equipment) inside the OT network;

• Use solutions designed to analyze network traffic, detect and prevent network attacks – at the boundary of the enterprise network and at the boundary of the OT network;

• Use dedicated solutions to monitor and perform deep analysis of network traffic on the OT network and detect attacks on industrial equipment;

• Ensure the security of hosts on the enterprise's IT and OT networks using solutions that provide protection from malware and cyberattacks.

• Provide cyber-hygiene training to employees, partners and suppliers who have access to the enterprise's OT network.

• To assist companies in choosing OT security solutions, world’s leading research and advisory company Gartner has released its Competitive Landscape: Operational Technology Security report (Authored by: Ruggero Contu, Published on: 29 October 2018). Kaspersky Lab was cited for its solutions under the following categories: OT endpoint security, OT network monitoring and visibility, anomaly detection, incident response, and reporting, and OT Security Service. To see the full complimentary copy of report please visit the Gartner website.

Read a complimentary copy of the full version of the report on the Kaspersky Lab ICS CERT website. https://ics-cert.kaspersky.com/reports/2019/01/14/security-research-thingspro-suite-iiot-gateway-and-device-manager-by-moxa/