Trend Micro Research Reveals Serious Vulnerabilities in Critical Industry 4.0-IT Interfaces

Protocol gateways prove critical for smart industrial environments

DALLAS, Aug. 5, 2020 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released research revealing a new class of security vulnerabilities in protocol gateway devices that could expose Industry 4.0 environments to critical attacks.

Also known as protocol translators, protocol gateways allow machinery, sensors, actuators and computers that operate in industrial facilities to talk to each other and to IT systems that are increasingly connected to such environments.

"Protocol gateways rarely get individual attention, but their importance to Industry 4.0 environments is significant and can be singled out by attackers as a critical weak link in the chain," said Bill Malik, vice president of infrastructure strategy for Trend Micro. "By responsibly disclosing nine zero-day vulnerabilities with the affected vendors, Trend Micro is leading the way with industry-first research that will help to make global OT environments more secure."

Trend Micro Research analyzed five popular protocol gateways focused around translation of Modbus, one of the most widely used OT protocols globally.

As detailed in the new report, vulnerabilities and weaknesses found in these devices include:

- Authentication vulnerabilities allowing unauthorized access
- Weak encryption implementations allowing decryption of configuration databases
- Weak implementation of authentication mechanisms resulting in disclosure of sensitive information
- Denial of Service conditions
- Flaws in the translation function that could be used to issue stealth commands to sabotage operations

Attacks leveraging such weaknesses could allow malicious hackers to view and steal production configurations and sabotage key industrial processes by manipulating process controls, camouflaging malicious commands with legitimate packets, and denying process control access.

The report makes several key recommendations for vendors, installers and end users of industrial protocol gateways:

- Consider the design of products carefully before selection. Ensure they have adequate packet filtering capabilities, so that devices aren't prone to translation errors or denial of service
- Do not rely on a single point of control for the security of the network. Combine ICS firewalls with traffic monitoring for improved security
- Spend time on configuring and protecting the gateway — use strong credentials, disable unnecessary services and enable encryption where supported
- Apply security management to protocol gateways as any other critical OT asset, i.e. regular assessments for vulnerabilities/misconfiguration, and regular patching

The results of this research will be presented at Black HatUSA on August 5. To find out more and read the full report, please visit: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/lost-in-translation-when-industrial-protocol-translation-goes-wrong.

About Trend Micro

Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers with connected solutions across cloud workloads, endpoints, email, IIoT, and networks.

Our XGen™ security strategy powers our solutions with a cross-generational blend of threat-defense techniques that are optimized for key environments and leverage shared threat intelligence for better, faster protection.

With over 6,700 employees in 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world www.trendmicro.com.

SOURCE Trend Micro Incorporated

For further information: Erin Johnson, 817-522-7911, media_relations@trendmicro.com

https://newsroom.trendmicro.com/2020-08-05-Trend-Micro-Research-Reveals-Serious-Vulnerabilities-in-Critical-Industry-4-0-IT-Interfaces