Trend Micro Research Reveals Dangerous Design Flaws and Vulnerabilities in Legacy Programming Languages

Cybersecurity leader and Politecnico di Milano jointly release essential guidelines for secure OT development

DALLAS, Aug. 4, 2020 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced new research highlighting design flaws in legacy languages and released new secure coding guidelines. These are designed to help Industry 4.0 developers greatly reduce the software attack surface, and therefore decrease business disruption in operational technology (OT) environments.

Conducted jointly with Politecnico diMilano, the research details how design flaws in legacy programming languages could lead to vulnerable automation programs. These insecurities could enable attackers to hijack industrial robots and automation machines to disrupt production lines or steal intellectual property. According to the research, the industrial automation world may be unprepared to detect and prevent the exploitation of the issues found. Therefore it is imperative that the industry start embracing and establishing network-security best practices and secure-coding practices, which have been updated with industry leaders as a result of this research.

"Once OT systems are network-connected, applying patches and updates is nearly impossible, which makes secure development upfront absolutely critical," said Bill Malik, vice president of infrastructure strategies for Trend Micro. "Today, the software backbone of industrial automation depends on legacy technologies that too often contain latent vulnerabilities, like Urgent/11 and Ripple20, or varieties of Y2K-like architectural defects. We don't want to simply point out these challenges, but once again take the lead in securing Industry 4.0 by offering concrete guidance for design, coding, verification, and on-going maintenance, along with tools to scan and block malicious and vulnerable code."

Legacy proprietary programming languages such as RAPID, KRL, AS, PDL2, and PacScript were designed without an active attacker model in mind. Developed decades ago, they are now essential to critical automation tasks on the factory floor, but can't themselves be fixed easily.

Not only are vulnerabilities a concern in the automation programs written using these proprietary languages, but researchers demonstrate how a new kind of self-propagating malware could be created using one of the legacy programming languages as an example.

Trend Micro Research has worked closely with The Robotic Operating System Industrial Consortium to establish recommendations to reduce the exploitability of the identified issues[1].

"Most industrial robots are designed for isolated production networks and use legacy programming languages," said Christoph Hellmann Santos, Program Manager, ROS-Industrial Consortium Europe. "They can be vulnerable to attacks if connected to, for example, an organisation's IT-network. Therefore, ROS-Industrial and Trend Micro have collaborated to develop guidelines for correct and secure network set-up for controlling industrial robots using ROS."

As these new guidelines demonstrate, the task programs that rely on these languages and govern the automatic movements of industrial robots *can* be written in a more secure manner to mitigate Industry 4.0 risk. The essential checklist for writing secure task programs includes the following:

- Treat industrial machines as computers and task programs as powerful code
- Authenticate every communication
- Implement access control policies
- Always perform input validation
- Always perform output sanitization
- Implement proper error handling without exposing details
- Put proper configuration and deployment procedures in places

In addition, Trend Micro Research and Politecnico diMilano have also developed a patent-pending tool to detect vulnerable or malicious code in task programs, thus preventing damage at runtime.

As a result of this research, security-sensitive features were identified in the eight most popular industrial robotic programming platforms, and a total of 40 instances of vulnerable open source code have been found. One vendor has removed the automation program affected by a vulnerability from its application store for industrial software, and two more have been acknowledged by the maintainer, leading to fruitful discussion. Details of the vulnerability disclosures have also been shared by ICS-CERT in an alert to their community[2].

The results of this research will be presented at Black Hat USA on August 5, and at the ACM AsiaCCS conference in October in Taipei.

To find out more, please find the complete research report here:https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/unveiling-the-hidden-risks-of-industrial-automation-programming.

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.

[1] https://rosindustrial.org/news/2020/6/23/how-to-securely-control-your-robot-with-ros-industrial
[2] https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-20-217-01

SOURCE Trend Micro Incorporated

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

---

https://newsroom.trendmicro.com/2020-08-04-Trend-Micro-Research-Reveals-Dangerous-Design-Flaws-and-Vulnerabilities-in-Legacy-Programming-Languages