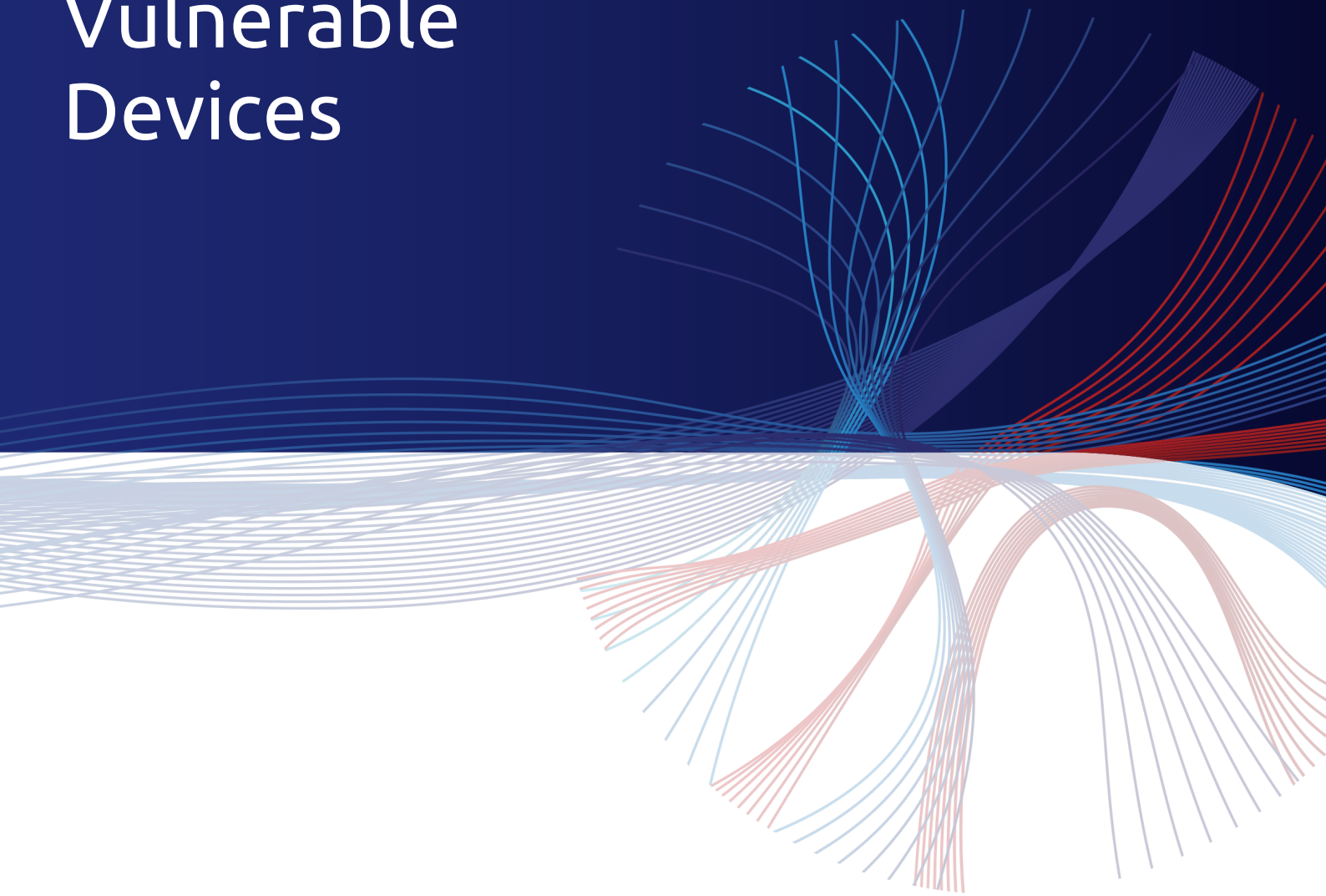
SCADAfence

Whitepaper

OT Cybersecurity for Inherently Vulnerable Devices



Introduction

The vast majority of Industrial Control System (ICS) devices are legacy devices that have been operating for years or decades — according to research by NIST, 85 percent of ICS devices in the field are more than ten to fifteen years old. Many, such as Programmable Logic Controllers (PLC), process sensors, gateways, and workstations are no longer patchable and cannot be upgraded due to technical or operational constraints. They present a significant cyber security challenge and pose serious risks.

The United States Council of Economic Advisors estimates that malicious cyber activity costs the U.S. economy between $57 and $109B per year. The NotPetya attack alone cost more than $1B, as A.P. Moller-Maersk and FedEx experienced an estimated $300M each in damages. More recent vulnerabilities such as Wind River VxWorks' Urgent11 and Schneider Electric TRITON/TRISIS revealed weaknesses that compromised the safety and reliability of control systems.

OT networks often control critical systems and processes and have both critical services as well as safety aspects. Therefore, it is crucial to reduce the level of exposure of these devices to external threats. Thus, it is critical to identify and manage vulnerabilities of the OT devices that control these critical processes.

However, OT devices are considered to be much more vulnerable than typical IT equipment for a few reasons:

- 1) Many OT devices have been designed tens of years ago with the assumption of air gapped networks, and were designed with little to no security considerations.
- 2) OT devices often do not have significant computational resources; therefore, OT processes are not open for security processes (e.g., timely verification checks, authentication processes, etc.) Therefore, little to no security measures have been implemented.
- 3) Many OT devices are less likely to be open to updates and patches, and/or are limited to legacy operating systems, and as a result, are more susceptible to exploits.
- 4) All the aforementioned reasons cause OT devices to have vulnerabilities for much longer periods of time.

The delicate nature of OT devices emphasizes an even more urgent need to properly analyze and discover the vulnerabilities of OT devices, and protect against them. However, detection of OT vulnerabilities is also not as simple as it sounds:

- 1) Due to process availability considerations, OT devices are much less open to scanning and testing routines, and therefore might contain hidden vulnerabilities that remain undiscovered.
- 2) The OT equipment industry has still not reached the level of maturity of the IT world. That's why some vendors do not cooperate in the research and disclosure of their equipment's vulnerabilities and do not add their vulnerabilities to the CVE database. This also contributes to the amount of hidden vulnerabilities that lie in these devices, and adds to the risks to the OT networks.

The day-by-day reality then, is that alongside the known and addressable (patchable) vulnerabilities, there exist many vulnerabilities that are either known but remain un-addressed for long period of times, or even worse, that remain hidden and undocumented. This means that no CVEs are being listed and managed, resulting in critical processes in OT networks to remain highly exposed to malicious actors.

How Inherently Vulnerable Devices Can be Protected

Patching to the Latest Available Version

While CVEs are not always available, as indicated above, it is recommended to patch to the latest available version from the equipment vendor.

Asset Identification, Visibility, and Management

There are a number of approaches to asset identification and visibility. Note, however, that some can be time consuming, costly, error prone, and risky. To improve visibility and detect unauthorized traffic and malware, organizations should implement passive scanning. Using passive network monitoring solutions can identify assets accurately, safely, and cost effectively. Asset identification and visibility should be used to define the architecture and network segmentation and to secure processes and procedures for managing and updating inventories and potential device vulnerabilities.

Risk Analysis and Security Planning

This begins with creating a map of the network and defining the criticality of assets and processes. This also helps organizations to learn the traffic patterns in their network.

This lets organizations understand the exposure that their processes are exposed to, and the level of risk from various possible events (accidental (failures, misconfigurations) and deliberate (malware, hacking attempts, etc.).

The risk analysis and security planning process, enables organizations to define their security architecture and tools such as network segmentation, remote access procedures, and enables them to reduce their risk.

Handling OT Network Exposures

One of the most important aspects in OT networks is to adhere to best practices – both architecture-wise, and traffic-wise.

Detecting and addressing the use of insecure protocols, insecure communications, the overriding of installed security tools, and other existing exposures in the network, can greatly improve health and security of the network. It also prevents damages from malicious attacks, even if no specific CVE is known ahead of time.

Detection and Handling of Zero-Day Threats

Not all threats are known and have CVEs or signatures. Attackers constantly innovate and change their behavior in order to override security tools, and to keep their malware and techniques undetected.

Every asset owner and OT operator should have a security incident response team. Detection and incident response in an industrial OT environment are more complex than in IT environments. While blocking the source IP address of an attacking host rarely causes issues in IT networks, it is often not feasible in OT environments that rely on real-time network performance with minimal delay. However, strong monitoring functions in OT allow tapping into a safety culture that can be used to respond quickly to operational incidents.

An organization should develop its own playbook depending on its needs and relevant risk ratings. Stakeholders should establish clear incident response policies and procedures. They should also perform periodic drills to test the effectiveness of their processes and review them regularly to ensure they are updated to account for new threats and their corresponding responses.

Incident Management

Not all security incidents can be prevented ahead of time. This enhances the importance of early threat detection and a rapid response.

When dealing with Incident Management in OT networks, it is important to maintain the process availability and safety, during the incident handling.

The recommended way is to have the detection tools integrated with a SOAR platform. There should have clear, predefined playbooks in order to handle many different types of alerts. It is also important to define in which cases, human intervention should be required and which cases should not.

It is also recommended to choose flexible threat detection platforms, with wide APIs, rather than with pre-defined and GUI managed integrations. Usually, pre-defined / GUI managed integrations are not flexible enough and do not meet the organizational requirements.

In Summary

Inherently vulnerable devices pose a substantial risk factor in industrial environments. Protecting them is critical to managing cyber security in OT systems. The growth of IIoT and Industry 4.0 is increasing the attack surface by connecting previously closed networks to the Internet. To protect systems, organizations need to contend with a variety of unique and frequently changing conditions, including unpatchable software, unsupported operating systems, insecure protocols, and unknown CVEs.

To respond to these challenges, organizations should adopt the cybersecurity recommendations and implementation guidelines presented in this white paper. These practical guidelines will help protect inherently vulnerable devices against cyber-attacks that compromise the safety and reliability of OT systems.

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cybersecurity. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access, and IoT device security. A Gartner "Cool Vendor" in 2020, SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing, and building management industries to operate securely, reliably, and efficiently. To learn more, visit our website, check out our blog, or follow us on LinkedIn.

NEW YORK,462 W Broadway New York, NY 10012, USA +1-646-475-2173

MUNICH, Schellingstr. 109a 80798 Munich Germany +49-322-2109-7564

TEL AVIV, 4 Menorat Ha'Maor St. Tel Aviv 6744832, Israel +972-3-763-0785

TOKYO, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Tokyo 103-0023, Japan +81-3-4588-5432

Contact us: info@scadafence.com

SCADAfence