TuxCare
We Take Care of Linux

WHITEPAPER

Industry 4.0 Live Security Patching

www.tuxcare.com

Operational Technology (OT) Has Undergone Fundamental Changes

The adoption of Industry 4.0 technologies into production facilities and throughout operations, such as automation, 3D printers, cloud computing, robotics, machine learning, and IIoT devices, is gaining momentum across smart manufacturing.

Industry 4.0 and OT Security Transformation

Also known as smart manufacturing, Industry 4.0 is the digital transformation of how organizations produce, enhance, and distribute their products. Now, “smart factories” are outfitted with advanced sensors and robotics, which enable manufacturers to collect and analyze data, increase automation, gain unprecedented levels of visibility, and reach new levels of efficiency.

With the rise of Industry 4.0 comes an increase in the number of connected machines. Industry 4.0 aims to combine the digital and physical worlds by marrying them together through smart, autonomous technology supporting the manufacturing industry.

These connected devices interface with the production lifecycle, enabling businesses to improve productivity and competitiveness through cost control and planning. There are five main characteristics of Industry 4.0 industrial environments, essentially serving as the vision of Industry 4.0 and helping guide companies wishing to understand, identify, and implement Industry 4.0 projects.

The 5 Characteristics of Industry 4.0 Industrial Environments:

Interoperability
Devices sharing standard protocols for intercommunication

Virtualization
Optimizing processes and anticipating changes by running “what if” scenarios through a virtualized model of production facilities

Decentralization
Industry 4.0 adoption of machines executing automated decisions

Real-time Analysis and Capacity
Adoption of automated data feeds from advanced sensors for faster decision making and problem resolution

Service-Oriented Delivery Model
Faster adoption of change, resulting in AI and ML data processing, creating faster adaptation as well as product and service delivery.

The concept of Industry 4.0 encompasses and extends the Industrial Internet of Things (IIoT) into the physical realm. The movement of digital technologies underpins the digital factory and digital service networks (DSN) enterprises' architecture.

The Threat Landscape of OT/ICS/IIoT/Industry 4.0

Traditionally, Operational Technology (OT), industrial control systems (ICS), and industrial devices were built into an air-gapped environment, where no network connection exists between the OT systems and any external systems. But today, connected factories and smart factories are implementing new digital technologies within their operations, such as intelligent sensors, connected IoT devices, and advanced analytics. While these more recent digital tools increase efficiency, lessen human intervention, reduce costs, and link disparate parts of the business, they also introduce new security vulnerabilities.

Due to the demand for digitalization, these formerly separated systems are now exposed. Attackers are increasingly targeting advanced manufacturing systems, and the ability to affect or shut them down provides them tremendous power. Information technology opens the door to new opportunities and introduces a vast landscape of cybersecurity threats.

OT environments have a lot of diversity in systems that OT industrial asset owners need to work with. And the job becomes even more complicated when ICS, such as DCS, SIS, programmable logic controller (PLC), etc., are installed by multiple vendors in the OT environment. This is why a practical patch management approach is essential to identify vulnerabilities and reduce risk to an acceptable level before attackers find them.

Developing a Patch Management Strategy for Industry 4.0

According to industry standards like IEC 62443, you should establish a patch deployment process and implement other cybersecurity strategies. It is suggested to have a baseline, record, review, document, and rollback (BRRDR) process when applying patches to the production environment, and we suggest using The Top 7 Operational Technology Patch Management Best Practices from ISA Global Cybersecurity Alliance. Since updating the production environment is considered a major operation, it is suggested to follow the same BRRDR process when using updates.

The national vulnerability database (NVD) releases more than

350

new threats

every week

The national vulnerability database (NVD) releases more than 350 new threats every week. It is difficult for OT asset owners to identify if all the threats and fixes apply to them. An automated solution, like PAS Vulnerability Assessment asset management updated daily with new threats and fixes, will help check in-depth inventories against the latest threats and fixes.

Identifying threats passively is a considerable benefit for OT asset owners, which can be done using solutions that compare current OT inventories to NIST's CWE database and ICSA-CERT advisory to find which assets are vulnerable and what fixes exist.

After identifying a threat, it must be evaluated as to whether it can be mitigated more effectively. For example, if a browser vulnerability is found in ten IT assets before the fix is deployed, the question would be whether Google Chrome is needed in all the ten IT assets. Removing it from some of the IT assets will mitigate the risk and reduce costs while deploying the fix.

TuxCare's Role in Live Patching Critical Hosts and Applications for Industry 4.0

Factories are transforming their systems to align with industry 4.0 standards, and more platforms, including AI and ML, cloud-based computing, and industrial robotic controls, require security updates.

The challenge is similar to the legacy OT/ICS platforms; many of these systems can not be taken offline for a maintenance window. Fortunately, with live patching technology from TuxCare, connected devices and smart factory ecosystems can automatically receive the latest Linux security patches without needing to perform system reboots or schedule maintenance windows.

Live security updates from TuxCare extend their legacy of rapid, automated IT security patching into the Industry 4.0 market. By offering live patching of critical-based Linux operating systems, open-source databases, and critical software libraries without requiring reboots, SecOps requirements can be more easily fulfilled within connected factories.

Support for Outdated Operating Systems in Smart Factories

Another critical challenge from OT/ICS is legacy support for automation applications and website portals – as many connected production facilities are still running operating systems past their vendor-supported lifecycles.

TuxCare's Extended Lifecycle Service (ELS) provides clients with ongoing security patches for Python 2.7, PHP, as well as a number of Linux distributions that have reached end of life (EOL) and no longer receive patches from their manufacturers. TuxCare ELS ensures your outdated operating systems receive security support for up to four years past their EOL date.

Now, you can continue to use existing Python 2.7 software on AlmaLinux, Rocky, or Red Hat Enterprise Linux 9 securely. The TuxCare ELS program for Python 2.7 enables you to continue using your existing software as before on a modern platform that satisfies your compliance requirements. At the same time, you receive security updates for high and critical vulnerabilities.

Closing the Linux Security Loophole Inside of Industry 4.0

You can automatically update Linux applications and kernels for industry 4.0 hosts by combining a scheduling program, like cron, with your platform's package maintainer, such as yum, apt, or dnf. Some Linux vendors have created packages that do unattended updating for you. And, as with everything in Linux, each flavor does it differently.

Debian and **Ubuntu** have the unattended-upgrades package

Fedora has DNF-automatic for automatic updates

Red Hat offers yum-cron (only available through the supplementary channel, in other words, for a fee)

However, anyone using these without reconfiguring the settings is likely to get a shock at some point:This is because, unlike applications, unattended updates don't mean you can install kernel updates without rebooting.

There's a security loophole. No organizations want to reboot servers. It's why kernels are excluded in unattended updates. They are vulnerable and vulnerable kernels are prone to exploitation.

Why TuxCare?

TuxCare is a global leader in open-source security, providing unmatched expertise in patching for your entire Linux estate. We deliver security patches to popular Linux distributions, end-of-life systems, programming languages, and more – offering a comprehensive security solution for all your infrastructure needs.

With over 80,000 patches – and counting – delivered to our users, TuxCare's solutions reduce vulnerability exposure, minimize downtime, eliminate patching-related disruptions, secure your open-source supply chain, and maintain system stability and compliance.

TuxCare protects the world's largest enterprises, government agencies, service providers, universities, and research institutions, safeguarding over a million workloads (and growing). Our mission is to drive continuous innovation through open-source technologies while minimizing the risk of cyber threats and serving as a trusted technology partner for innovative organizations across the globe.

LEARN MORE AT
www.tuxcare.com