INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

September 2021

Upcoming Events

ICSJWG Webinar

Join us on **October 20th from 1 PM to 2:15 PM eastern time** for the upcoming ICSJWG "End of Life/End of Support Considerations for Industrial Control Systems Webinar." *For more information on the upcoming webinar please go to the ICSJWG website, CISA.gov/ICSJWG.*

ICS Evaluation (401v & 301v) Online Virtual Training

Industrial Control Systems Evaluation (401v) Online Virtual Training
October 4 to 22

Course information and registration

CISA Resources

CISA ICS Security Offerings
Training Resources
Incident Reporting
Assessments
CSET®
Alerts
Advisories
HSIN
Information Products

Thank you to everyone who submitted content for this newsletter. ICSJWG relies on members like you for our Newsletter, Meetings, and Webinars. Content and opinions are those of the authors and do not represent DHS opinions, endorsements, linguistic styles, or recommendations.

Thanks for attending!

The ICSJWG 2021 Fall Virtual Meeting - Recap

On September 21st and 22nd, CISA presented the fourth virtual version of the Industrial Control Systems Joint Working Group (ICSJWG) bi-annual event, the ICSJWG Fall 2021 Virtual Meeting. We featured a welcome greeting video from CISA Director Jen Easterly that inspired the audience to participate with CISA. We kicked off the meeting with a keynote by Acting Associate Director for Threat Hunting, Alexis Wales, titled "ICS Public Private Partnership – Taking It to the Next Level." Day 2 started with Aaron Boyd and Francesca Brogden from Dragos speaking about "Living Off the Land in an ICS/OT Penetration Test."

On Day 1, ICS subject matter experts and ICSJWG partners delivered technical presentations concerning the cybersecurity of our critical infrastructure. We had an in-depth introduction to the CSET Ransomware module and an update about the Control Systems Working Group. Day 2 continued with presentations speaking to the CDET CYBER-CHAMP© training, to facilitate making our systems more secure and our workers more cyber-knowledgeable. We welcomed back Technical Workshop: Treating the Cybersecurity Testbed, Software Bills of Material, and Cost Effective SIEM.

The always popular and instructive "Capture the Flag" activity was held for the participants over both days.

The ICSJWG meeting had representation from all 16 sectors, 57 countries and 48 U.S. states. If you missed the opportunity to participate, click here to access the recorded webcasts. For additional information, please contact us at ICSJWG.Communications@cisa.dhs.gov.

CISA Announces 4th Annual National Cybersecurity Summit

CISA is excited to announce the return of the CISA Annual National Cybersecurity Summit for its fourth year! Last year's Cyber Summit was hosted online as a series of four weekly, virtual events, drawing more than 15,000 attendees. The 2020 Cyber Summit educated external participants on the threats, roles, and actionable steps to take toward maintaining cybersecurity.

This year, we're hosting our Annual National Cybersecurity Summit virtually yet again. We are excited to continue the legacy of CISA's Cyber Summit and continue to provide a forum for meaningful conversation about cybersecurity and collaboration toward collective action.

The 2021 CISA Annual National Cybersecurity Summit will be held virtually as a series of webinars every Wednesday in October, beginning October 6 and ending October 27. The virtual Cyber Summit will be hosted on Microsoft Teams Live and can be viewed at cisa.gov/live.

Each week will have a unique theme. This year's themes are:

- Oct 6: Assembly Required: The Pieces of the Vulnerability Management Ecosystem
- Oct 13: Collaborating for the Collective Defense
- Oct 20: Team Awesome: The Cyber Workforce
- Oct 27: The Cyber/Physical Convergence

For registration and more information, visit cisa.gov/cybersummit2021.

CISA Releases Two ICT Supply Chain Resources to Improve Information Sharing and Assist Small and Medium-sized Businesses

The Cybersecurity and Infrastructure Security Agency (CISA) released two new products developed by the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force to address liability challenges on sharing supply chain threat information and assist Small and Medium-sized Businesses (SMBs) with mitigating ICT supply chain risks.

Improving the quality and volume of supply chain risk information sharing among the federal government and private industry is necessary to obtain actionable information that could mitigate threats to the Nation's ICT supply chain. Building off work completed in Years 1 and 2, the Task Force's Information Sharing Working Group (WG1) developed the Preliminary Considerations of Paths to Enable Improved Multi-Directional Sharing of Supply Chain Risk Information, which offers subject matter expert research on legal and policy considerations for giving liability protection to the federal government and private sector in order to promote information sharing.

In January 2021, the Task Force launched three new WG efforts including the SMB WG, which was created to tailor Task Force products to make them more accessible, relevant, and usable for SMBs. The Operationalizing the Vendor SCRM Template for SMBs helps IT and communications SMBs assess their ICT supply chain risk posture when procuring new ICT hardware, software, and services or acquiring new contracts from the perspective of the acquirer, integrator, and supplier. Additionally, this guide includes an easy-to-use spreadsheet as an alternate tool. Both products gear the applicability of the previously released enterprise Vendor SCRM Template to help SMBs apply industry standards and best practices in a standardized way.

The Task Force embodies CISA's collective defense approach to enhance ICT supply chain resilience. In two years, it has developed a variety of SCRM products; an online SCRM toolkit with strategic messaging and videos; and comprehensive webpage with free and voluntary SCRM resources and information from across the federal government. Moving forward, the Task Force will continue to leverage its collective expertise to develop actionable solutions on a wide range of supply chain issues.

For these resources and more, please visit: CISA.gov/ict-supply-chain-toolkit. Additionally, please read our latest blog article, *Sharing Information to Get Ahead of Supply Chain Risks*, and view the videos below.

Mitigating ICT Supply Chain Risk for Small and Medium-sized Businesses - YouTube

Improving Multi-Directional Sharing of Supply Chain Risk Information - YouTube

CISA Releases Infrastructure Resilience Planning Framework

The Infrastructure Resilience Planning Framework (IRPF) is a framework that enables users to identify critical infrastructure, assess related risks, and develop and implement resilience solutions. The framework helps them understand interconnected infrastructure systems and can be incorporated into many types of plans such as economic development, capital improvement plans, hazard mitigation, and emergency response/recovery. The IRPF's audience is state, local, tribal, and territorial governments, regional planning commissions, infrastructure owners and operators, and large manufacturing clusters.

The IRPF outlines five key steps that can be incorporated into existing planning processes to enhance resilience by addressing critical infrastructure dependencies. To support these steps, it includes guidance, tools, and resources such as infrastructure dependency questions, a meeting facilitation guide, and a compendium of mechanisms to fund resilience solutions. The draft IRPF was piloted and improved in collaboration with the Commonwealth of Kentucky and CISA Region IV over the past two years. It has also been reviewed by other stakeholders such as FEMA.

Are there other related resources?

CISA/ISD is developing additional resources to supplement the IRPF.

- The Infrastructure Dependency Primer is a video series describing the fundamentals of interconnected infrastructure systems. It was developed based on state and local comments that users might not be aware of these concepts, which are useful when applying the IRPF. We expect the Primer to be posted to CISA's website this November.
- ISD is close to completing the Drought and Infrastructure Planning Guide, a brief resource describing the impacts and considerations of drought on infrastructure systems. We expect the Guide to be released around November as well.
- Additionally, ISD is preparing to publicly release the Regional Resiliency Assessment Methodology, which provides a framework for conducting regional infrastructure assessments based on lessons learned from the Regional Resiliency Assessment Program. The Methodology can be used to support the assessment phase of the IRPF.

Questions, Comments, and Follow-ups

If you have questions, comments, or would like to receive a presentation, feel free to email us at idr@cisa.dhs.gov. You can also contact David Willey (David.Willey@cisa.dhs.gov) or Sandra Pinel (sandra.pinel@cisa.dhs.gov). We are also available to present at any meeting you are scheduling.

Continue to IRFP Fact Sheet...

CISA Launches Insider Risk Mitigation Self-Assessment Tool

Insider threats pose significant risk to the safety and security of America's critical infrastructure and the organizations that keep infrastructure operational.
Organizations have a duty to protect themselves and their employees from unnecessary physical and cyber risks. Managing, detecting, and preventing insider risk is everyone's responsibility, and it is critical that efforts to manage that responsibility are tailored to each organization's environment and its mission's unique nature.

Recognizing the complexity of this threat, CISA is pleased to announce the Insider Risk Mitigation Self-Assessment Tool, available at cisa.gov/publication/insider-risk-self-assessment-tool.

The tool is a fillable PDF that asks users key questions about their existing enterprise, focusing on the areas of Program Management, Personnel and Training, and Data Collection and Analysis. The interactive PDF will allow users to fill in their data and receive scores representing maturity indicators that objectively evaluate their immunity to insider threat incidents; the response also includes guidance to interpret the numbers and provide suggested measures.

The self-assessment tool is another way CISA is working together with public and private stakeholders at the federal, state, local, and community levels to prevent and mitigate risks to our nation's critical infrastructure.

Additional information on critical infrastructure security and resilience is available on our website: cisa.gov/infrastructure-security.

Contributed Content Disclaimer:

vendors based on their business and security needs. This is of great importance because, at present, developers are left to sort through numerous message formats and supporting sets of protocols in order to first determine what should be implemented, and then to define how to secure it.

The guide will consolidate this information in one place and will offer consensus-validated recommendations in order to enhance the decision-making process and to improve the overall security posture of IoT devices. The end result will be more detailed benchmarks and recommendations when implementing data transport protocols for IoT solutions. Vendors will have unique and specific guidance on the best IoT protocols that provide built-in security. Installing embedded security on devices at the vendor level will ultimately enhance the cybersecurity of critical infrastructure.

CIS initiated these efforts prior to the release of President Joe Biden's "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems," on July 28, 2021. The presidential memorandum was released in the wake of multiple cyber-attacks targeting U.S. critical infrastructure and calls for participation from the critical infrastructure community to improve the security of critical systems. It also builds on the February 2013 Executive Order 13636 (Improving Critical Infrastructure Cybersecurity). It is not practical to secure devices at each organization, hence the call for built-in security in these recent executive orders.

We are asking the ICSJWG community for industry experts and interested parties to participate in the CIS **IoT Embedded Security Working Group** to contribute to the review process of this groundbreaking project and to refine the recommendations prior to publication. If you are interested, please send your contact information and references to Ben.Carter@cisecurity.org. As an ICSJWG Member, we will also be hosting an ICSJWG webinar on this effort highlighting the guidance draft and conducting open dialog among those who may be interested in ongoing participation.

Your involvement and contributions will strengthen the guidance needed for vendors to install built-in security on IoT devices and sort through the options available more easily. Providing IoT vendors with this publication will help streamline industry security standards and set a framework for how devices are developed moving forward, which will be vital to the security of systems in the United States.

Continue to full article…

ICS Cyber Defense Must Match the Industrial Process

By: Daniel Ehrenreich, Consultant and Lecturer, SCCE

ICS-OT-IIoT terms are broadly used for controlling industrial and utility applications. Their architecture may be complex or simple, involve many or just few installations and use serial, ethernet or wireless media for connecting a broad range of sensors and actuators with on-site control. While IT operations are protecting Data, Privacy and money through the CIA Triad, most industrial operation must protect Safe and Reliable operation and Business Continuity via the SRP Triad (Safety-Reliability-Productivity).

Consequently, these ICS-OT-IIoT operations must be defined and designed according to the criticality of the on-site process. In some cases, the cyber security requirements may be light and in other projects for a similar application the specification can be tougher and more complex.

In recent years we see the penetration of IIoT ecosystems to ICS-OT-IIoT enhance with a goal to enhance the business performance, while disregarding the risky increase of the cyber-attack surface. Furthermore, many cyber security experts are already aware of an incorrect (probably never defined) term "IT-OT Convergence" which has been adopted by some security practitioners, sales & marketing, press & media, and some business units' managers who believe in benefits by converging the IT and OT networks.

In a correctly designed architecture, the ICS-OT-IIoT cyber defense shall be defined according to assessment as outlined in section 3-2 of the ISA-IEC 62443 standard or in a similar document used worldwide. The system architect must deal with factors such as operation safety, reliability, performance, data integrity, operation convenience and last but most important with cyber security.

Continue to full article…

The U.S. Government does not endorse any specific commercial products, processes, or services. Any opinions or comments by commercial entities are provided for informational use only and do not imply an endorsement of any kind by the U.S. Government.

New Edition of Cybersecurity Standard for Pipelines Provides Comprehensive Approach to Cyber Defense for Critical Infrastructure

Provided by: Suzanne Lemieux

On August 18, 2021, The American Petroleum Institute (API) published its 3rd Edition of Standard (Std) 1164, *Pipeline Control Systems Cybersecurity*, underscoring the natural gas and oil industry's ongoing commitment to protecting the nation's critical infrastructure from malicious and potentially disruptive cyber-attacks.

In development since 2017, the 3rd edition is a result of expert input from more than 70 organizations, including state and federal regulators within FERC, TSA, PHMSA, CISA, DoE, NIST, as well as Argonne National Laboratory, the American Gas Association (AGA), Interstate National Gas Association of America (INGAA), the Association of Oil Pipe Lines (AOPL) and numerous pipeline operators. It is based on the NIST (National Institute of Standards and Technology) Cybersecurity Framework and NERC-CIP (Critical Infrastructure Protection) standards and significantly expands the scope compared to the previous edition of the standard to cover all control system cybersecurity instead of solely supervisory control and data acquisition (SCADA) systems.

"The new edition API Std 1164 builds on our industry's long history of engaging and collaborating with the federal government to protect the nation's vast network of pipelines and other critical energy infrastructure from cyber-attacks," API Senior Vice President of API Global Industry Services (GIS) Debra Phillips said. "This standard will help protect the nation's critical pipeline infrastructure by enhancing safeguards for both digital and operational control systems, improving safety and preventing disruptions along the entire pipeline supply chain. What sets this framework apart is its adaptive risk assessment model that provides operators with an appropriate degree of flexibility to proactively mitigate against the rapidly evolving cyber threat matrix."

"This premier standard helps the operator manage cyber-risks associated with control system cybersecurity environments by providing requirements and guidance for proper isolation of control system environments from non-control system environments," American Gas Association Senior Vice President for Safety, Operations and Security Christina Sames said.

This expansion of the standard supports the Biden administration's national security priorities as well as the United Nations Sustainable Development Goal (UNSDG) 9 for resilient infrastructure. The updated standard establishes requirements to harden pipeline cybersecurity assets against a range of threats, including those posed by ransomware. It provides enhanced protections at critical connection points along the supply chain, specifically at pipelines, terminals, and refineries. Additionally, it includes improved risk assessment guidelines, a comprehensive model for implementing pipeline cybersecurity, and a framework for building out a robust industrial automation control (IAC) security program as part of the U.S. Transportation Security Administration required corporate security program.

"API Std 1164 reflects state-of-the-art cybersecurity protections tailored specifically to pipeline operations," Association of Oil Pipe Lines President and CEO Andy Black said.

This new edition pairs with other API standards to form a framework that is integral to industry's ongoing work to counter cyber threats, including:

- API 780 – Provides tools to conduct effective security risk assessments, which are used to identify threats to facilities as well as countermeasures to those threats. Last October, API 780 was certified as an anti-terrorism technology by the U.S. Department of Homeland Security (DHS) under the Support Anti-terrorism by Fostering Effective Technologies Act of 2002. This provides liability protection if API members and others using API 780 have a terrorist attack at one of their facilities.

Recommended Practice 1173 – Pipeline Safety Management Systems provides pipeline operators with safety management system requirements that when applied provide a framework to reveal and manage risk, promote a learning environment, and continuously improve pipeline safety and integrity.

How to get things patched faster - CSAF 2.0 and the future of advisories

By: Jens Wiesner, BSI

It is not a novel insight that the number of discovered and treated vulnerabilities is constantly rising. As more vendors are dealing with coordinated vulnerability disclosure (CVD) and slowly discover their responsibility to maintain their products also the number of security advisories rises. Moreover, Software Bill of Materials (SBOMs) provide greater insights in the supply chain that will also add to the released advisories. And they will come, as President Biden demands their implementation in EO 14028.

Therefore, the real question is how to deal with it. Basically, there are 3 options:

1. Don't care about security advisories, 2. Try to manually process all security advisories,3. Automate security advisories. Let's have a look into each of them.

Don't care about security advisories

Instinctively many security professionals will say that this is a bad option. However, we should take a closer look as there are two ways: The first one is to ignore security advisories and the vulnerabilities described in them as well. After a short time, someone using that strategy ends up having a vulnerable system – and doesn't know anything about that. And that is really bad.

The second way is to rely on an auto-update function. This is far from perfect but an acceptable resp. accepted solution in IT when uptime is not an issue (might be treated differently with server systems). However, when it comes to Industrial Control Systems (ICS) nobody likes losing control over an update. The reason for that different mindset is the different importance of the security goal availability. In addition, some advisories go beyond installing of updates and require actions in form of configuration or other measures in the infrastructure.

Try to manually process all security advisories

Many are currently using this option. We evaluate the cyber risk for our environment or products by manually processing security advisories. However, this process is time and resource intensive and therefore expensive.

First of all, we need to become aware that a new advisory (or a new version of an existing advisory) has been published. We receive that information in various ways: via email, through RSS feeds, etc. Then, we need to retrieve the advisory and analyze whether it affects the products we are responsible for and what the impact is. Based on that impact assessment a decision for an action can be made and has to be documented. Unfortunately, ICS use hundreds of vendors and all of them have different wording, formats and structure for their advisories. Therefore, no easy comparison with an asset database can be done. All this is usually manual work and that doesn't scale at all!

Automate security advisories

Therefore, the international community developed in a joined effort as open standard under the umbrella of the OASIS Open Foundation the Common Security Advisory Framework (CSAF) Version 2.0. It is a JSON-based format for security advisories that will aid in automation of the process on both ends – advisory issuers as well as consumers of advisories.

Superseding the XML-based CSAF Common Vulnerability Reporting Framework (CVRF) 1.2 it also specifies the distribution and discovery of security advisories. Moreover, CSAF 2.0 defines the requirements for tools so that, hopefully in a few months, everyone can easily compare and choose from different tools available on the market.

As this can be applied throughout the supply chain, upstream vulnerabilities can be communicated downstream much faster as the process is automatable. Furthermore, it becomes also possible to explicitly state that one's product is not affected by using the VEX (Vulnerability Exploitability eXchange) profile. Such mechanism can help reduce the false positive rate from security scanners and more important support hotlines but actively informing the customer.

The solution of using a standardized form of machine-readable security advisories seems to be so easy, so natural that you might ask: Why don't we have that today?

The sad answer to that is: Nobody asked for it. But that is something you can change easily: email your suppliers, put it into the next call for bids or contract negotiation, offer it to your customers, discover the added-value for your company, twitter about it (please make sure to include #advisory #oCSAF),

Technical Committee members have already started to implement their security advisories in CSAF, including but not limited to Arista, Cisco, Microsoft, Red Hat, and Siemens.

The latest news about the standard and available open source tools can be found at https://csaf.io. If you have any questions, do not hesitate to reach out to the TC or BSI at csaf@bsi.bund.de.

2020 Report on Threats Affecting ICS Endpoints

By: Matsukawa Bakuei, Ryan Flores, Lord Remorin, Fyodor Yarochkin, Trend Micro

The security of Industrial Control Systems (ICS) has been pushed into the limelight over the past few years due to the increasing interconnection between the business process on the IT side and the physical process on the OT side. While this interconnection improves visibility, efficiency, and speed it also inadvertently exposes ICSs to threats that have been affecting IT networks for decades. To validate ICS security and establish a global baseline for examining the threats that plague these systems, we analyzed and reported specific malware families found in ICS endpoints. The type of malware cybercriminals chooses to wield in particular incidents offers a glimpse into the scope and severity of these cyberattacks, providing clues on two key aspects: the attackers and the affected network. The choice of malware helps unveil the attackers' motivation and skill level. For example, the use of ransomware or a coin miner signifies financial motivation, the use of a wiper or other destructive malware suggests sabotage, and the use of a backdoor or information stealing malware reveals espionage. In terms of the attackers' skill, the use of customized malware suggests high technical skill or understanding of the attacked environment, while off-the-shelf malware suggests amateur skills, although this is not always the case. The malware found in the system could also provide insights into the affected network's environment and cybersecurity hygiene. We can infer the inadequate security practices applied on the affected networks based on malware infections found in them. For one, malware variants exploiting certain vulnerabilities imply unpatched endpoints. On the other hand, file-infecting viruses suggest previous infections that were not totally eradicated, with groups of unchecked devices hosting the viruses. By identifying and breaking down the malware threats found in ICSs through the data we gathered in 2020, we hope to provide insights into the general security posture of industrial control systems found in IT/OT environments and what attackers are doing once they compromise it. We also share recommendations on how to secure these environments.

Continue to full article…

Minimizing Risk with FPGAs and Hardware-Based Security

By: Devin McCrate, OWL Cyber Defense

Conventional data security technology has entered a mode of persistent escalation. System designers invest heavily in design and validation, while attackers continually uncover, exploit, and share new vulnerabilities. The result is a stream of updates and patches to close known attack methods. To slow the evolution of new threats and protect vulnerable systems from malicious actors, a paradigm shift and a new approach is needed.

Hardware-based cybersecurity using field programmable gate array (FPGA) technology provides stronger, more cost-effective protection for devices used by critical infrastructure, military, and intelligence organizations. Unlike the CPUs that power software firewalls, FPGAs are limited to a finite number of possible states, greatly reducing the scope of potential implementation flaws or vulnerabilities.

Why hardware-based security? Guarantees and fundamental assurances are rare in cybersecurity. The goal is typically to find the solution that offers the lowest risk of compromise compared to other solutions, with the understanding that the risk will always be greater than zero.

Hardware-based security reduces security risk to the lowest possible level and gives organizations a high degree of confidence that their components cannot perform any functions other than the ones they were designed to perform.

While nothing can eliminate all cybersecurity risk, the addition of hardware security technology can turn previously vulnerable spots into the strongest points in a network and dramatically reduce an organization's attack surface.

Continue to full article…

The U.S. Government does not endorse any specific commercial products, processes, or services. Any opinions or comments by commercial entities are provided for informational use only and do not imply an endorsement of any kind by the U.S. Government.

Targeted Ransomware – Capabilities, not Probabilities

By: Andrew Ginter, VP Industrial Security Waterfall Security Solutions

The classic equation risk = consequence x likelihood works well for random events, such as earthquakes and hurricanes. The formula even works for random equipment failures and is used routinely in sophisticated safety case calculations. The formula is a harder fit for deliberate attacks, such as today's targeted ransomware. There is little about targeted attacks that is random. Once an attacker engages with a target, the attack either works or it doesn't. If the attack works, then that same attack will almost certainly work again when launched against the same target a second time, or a third time.

A more useful approach for modelling deliberate ransomware attacks comes from the method physical security teams use to model the risk of terrorist attacks. This approach models risk as a combination of consequence, intent, capability, and opportunity. In this model:

- Consequence is the undesirable event we are concerned about. The most common OT consequence of today's targeted ransomware groups is a plant shutdown, or more commonly the shutdown of several plants simultaneously.
- Intent is the attacker's goal - extortion in the case of ransomware attackers. Intent guides the attacker through a chain of attack opportunities.
- Capability is the tools, techniques, and other resources available to the attackers.
- Opportunity is any set of attack paths through our defensive systems that might lead an attacker to bring about the undesirable consequence.

Sophisticated, well-defended sites are applying this model successfully to ransomware and other targeted attacks, because these attacks, like terrorist attacks, are deliberate and intentional rather than accidental or random.

Continue to full article…

The Need to Change the Paradigm of Control System Cyber Security – Monitor Process Sensors

By: Joe Weiss, PE, CISM, CRISC, Applied Control Solutions, LLC, Rob Stephens, PhD, JDS Energy and Mining, Nadine Miller, ME, MBA, JDS Energy and Mining

With the never-ending, and too often successful, attacks on critical infrastructure networks, there needs to be a better way to protect control systems and the processes they monitor and control. On July 28, 2021, an announcement was made about the President’s Industrial Control System Cybersecurity (ICS) Initiative to facilitate the deployment of technology and systems that provide threat visibility, indicators, detections, and warnings. To date, this is a network-based approach specific to cyber threats. However, the existing approach of securing critical infrastructures by securing the networks alone is inadequate without being able to verify the process sensor measurement integrity (process anomaly detection). As an example, the ISA99 control system cyber security standards, like all other cyber security standards, assume process measurement integrity, without requiring assurance of process measurement integrity like is required for data. Assuring process measurement integrity provides predictive maintenance and process integrity as well as validity of the sensor input for cyber security. The Israel Water Authority recognized the need to monitor the sensor signals and is monitoring the electrical characteristics of the process sensors as the process sensors are ground truth and not susceptible to network attacks so long as the raw signals can be measured before any signal pre-processing occurs. Process sensor monitoring needs to be incorporated into the overall control system cyber security program to complement the network monitoring approaches. The US government, insurance companies, credit rating agencies, and others need to recognize what really needs to be secured – the field control system equipment that keeps lights on and water flowing.

Continue to full article…

Examining ICS/OT Exploits: Findings from More Than a Decade of Data

By: Jacob Baines, Principal Industrial Control Vulnerability Analyst Threat Intelligence, Dragos, Inc.

An exploit is considered ICS/OT-related when it can reasonably be determined to affect a system within an ICS/OT network. For some systems it is obvious. PLCs, HMIs, and Historians are ICS/OT-related. Likewise, products developed by Rockwell and Schneider Electric are likely to be ICS/OT-related. There are a lot of less obvious ICS/OT-related systems though. For example, Dragos customers have VPN appliances in their ICS networks and ICS-specific activity groups like PARISITE12 target them for Stage 1, initial access13. Similarly, Dragos's experience and the Oldsmar Water Treatment Facility incident14 show that remote desktop solutions are deployed in ICS networks. While VPN appliances and remote desktop solutions are not ICS-specific, it is reasonable to describe these systems as ICS/OT-related. Perhaps more controversial is how to handle Microsoft Windows Operating System (Windows OS) exploits. Many ICS/OT systems are deployed on top of Windows, and exploits like ETERNALBLUE15 (MS17-01016) have been used to infiltrate ICS/OT networks on a number of occasions17. We therefore include it in our data set even though it isn't an ICS/OT vulnerability per se. But not all Windows vulnerabilities are practical within an ICS/OT network. Currently, the only public Windows OS exploits included in our data set are unauthenticated, remote exploits affecting default services or services we deem reasonable to be present in an ICS network (for example, Remote Desktop).

This paper covers vulnerabilities published between 2010 and April 2021. Vulnerability publication can refer to a National Vulnerability Database17 (NVD) entry, a vendor advisory, a researcher advisory, or a third-party advisory such as those produced by Industrial Control Systems Computer Emergency Response Team18 (ICS-CERT). The contents of the CVEs in the data set are not restricted to CVEs issued from 2010 onwards. For example, an ICS-CERT advisory published in 201519 indicated that a Honeywell product was vulnerable to CVE-2007-648320. Although CVE-2007-6483 was originally published in 2007, the 2015 advisory proved it remained relevant to our 2010 to April 2021 timeline. As such, CVE-2007-6483 and the corresponding public exploit21 are included in our data set.

Continue to full article...