INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

March 2022

Upcoming Events

Save the date!

ICSJWG Spring Virtual Meeting, **April 26-27, 2022**.

Trainings:

Industrial Control Systems Cybersecurity (301v) Online Virtual Training

March 14-25

Course information and registration

Industrial Control Systems Cybersecurity (401v) Online Virtual Training

April 4-22

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.

The ICSJWG Spring 2022 Virtual Event - Save the Date!

Please save April 26- 27, 2022, in your calendars for the Spring 2022 Virtual Event. We will have two full days of presentations, panels, demonstrations, and technical workshops from subject matter experts. We are also excited to announce that the Capture the Flag event will start the week prior.

Spring Meeting Highlights:

- Keynote Presentation by CISA Deputy Director Natarajan
- Capture the Flag will start on April 16th and run through April 27th, providing more time to engage in the challenge.
- Threat Hunting Technical Workshop
- Cyber – CHAMP© Presentation

The meeting welcomes all Industrial Control Systems (ICS) community members from around the globe, including those new to the concepts and subject matter experts with years of experience. We look forward to virtually seeing you there and continuing to build our partnership with the ICS Community. For more information, please contacts us at: ICSJWG.Communications@Cisa.dhs.gov .

Apache Log4j Vulnerability Guidance

CISA and its partners, through the Joint Cyber Defense Collaborative, are responding to active, widespread exploitation of a critical remote code execution (RCE) vulnerability (CVE-2021-44228) in Apache's Log4j software library, Versions 2.0-beta9 to 2.14.1, known as "Log4Shell."

Log4j is very broadly used in a variety of consumer and enterprise services, websites, and applications—as well as in operational technology products—to log security and performance information. An unauthenticated remote actor could exploit this vulnerability to take control of an affected system. Organizations are urged to upgrade to Log4j 2.17.1 (Java 8), 2.12.4 (Java 7) and 2.3.2 (Java 6), and review and monitor the Apache Log4j Security Vulnerabilities webpage for updates and mitigation guidance.

CISA releases "Shields Up" Message regarding Geopolitical Tensions

Every organization in the United States is at risk from cyber threats that can disrupt essential services and potentially result in impacts to public safety. Notably, the Russian government has used cyber as a key component of their force projection over the last decade, including previously in Ukraine in the 2015 timeframe. The Russian government understands that disabling or destroying critical infrastructure—including power and communications—can augment pressure on a country's government, military, and population and accelerate their acceding to Russian objectives.

While there are not currently any specific credible threats to the U.S. homeland, we are mindful of the potential for the Russian government to consider escalating its destabilizing actions in ways that may impact others outside of Ukraine. Shields Up | CISA: Check this page for continuous updates.

We're Back! CISA Re-Opens Registrations for In-Person ICS Cybersecurity Training

The chance for in-person, hands-on learning of Control System risk reduction is BACK! CISA is offering a free cybersecurity workshop for ICS March 14-17 in Idaho Falls, Idaho, featuring unique exercises designed to teach real-time protection of critical network resources.

Attendees take part in a red team versus blue team exercise, conducted within an actual control systems environment, and have the chance to beat a series of cyber escape rooms. The workshop includes instructor-led, hands-on experience with open-source operating systems and security tools. Through it all, attendees will be networking and collaborating with other colleagues involved in operating and protecting critical infrastructure.

During the pandemic, CISA adapted to a virtual model to continue to offer this valuable course to the industry. The virtual courses are now available as prerequisites to support a more in-depth learning experience and help participants be better prepared for the in-person workshops.

The in-person workshop (301L & 401L) is now a companion course to the required virtual course on risk reduction for Industrial Control Systems (301V). The course is IACET accredited and awards Continuing Education Units (CEUs) and a certificate upon completion.

For more information or to register, please visit https://cisa.gov/uscert/ics/Training-Available-Through-ICS-CERT.

CISA looking to identify vendor partners to participate in Critical Product Evaluations

CISA has openings for Critical Product Evaluations (CPEs) and is looking to identify vendor partners to participate in these valuable free assessments. We would greatly appreciate your participation or any suggestions or recommendations for CPE partners you may have. The CPEs provide free testing of devices used in critical infrastructure to identify vulnerabilities or other security concerns, which are shared as confidential information with the vendor.

- We look for tangible solutions or appliances we can bring to the lab for testing.
- The vendors only need to pay the shipping/transportation costs to INL; the assessment is completed by CISA.
- We are not able to provide accreditations or certifications.
- We work to collaborate with the vendors to reduce the vulnerabilities to US CI.

- We do not publish the CPE results beyond the vendor and Federal Government; proprietary information is destroyed after the CPE.
- We do look for devices that have completed development and are being used in the US CI but can be updated so our recommended mitigations can be implemented.

If any vendor chooses to participate, please contact: vulnerability@cisa.dhs.gov

IST Steering Team seeking new candidates

Do you have an interest in becoming more involved with ICSJWG through an advisory role? The IST Steering Team is looking to fill a SLTT position within the team. For more information or to apply for the role, email the ICSJWG team: ICSJWG.Communications@Cisa.dhs.gov .

Securing OT against Log4j; Is it really a thing?

By: Marty Edwards, VP OT Security & Michael Rothschild, Senior Director, OT Solutions

By now, you are well familiar with CVE-2021-44228. The Log4j vulnerability is being categorized as one of the most pervasive and potentially far-reaching vulnerabilities in history. Log4j is an open-source Java logging library used extensively by developers. First appearances are that this is an IT issue that cannot impact OT environments; but in fact, Apache and thus Log4j is embedded in operational technology (OT) environments. In fact, many organizations have converged their IT and OT operations thereby making lateral creep of attacks between the two increasingly common. Even if your facility is fully air-gapped, there is a better than average chance that you may be "accidentally converged", thus putting your operation at risk.

Here are five key actions to take right now to secure your OT environment against Log4j:

1. **Follow official guidance**. Organizations such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) have issued specific guidance. It is crucial to be familiar and follow this guidance on an ongoing basis. Compliance with, and reliance on, frameworks from MITRE, the U.S. National Institute of Standards and Technology (NIST), the U.K. Network and Information Systems (NIS) and the North American Electric Reliability Corporation (NERC) can help your organization establish best practices in order to stay vigilant against dynamic threat conditions.
2. **Know your assets.** Asset inventory is a cornerstone of any security program and can provide deep situational awareness. It involves more than capturing the make-and-model of everything in your environment. It requires having an up-to-date inventory of firmware versions, patch levels, communication paths, access and much more. Network monitoring alone will only provide some of the detail. A combination of network and device-specific querying is necessary in order to get the specifics.

Continue to the full article

1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information

By: Daniel Kapellmann Zafra, Corey Hidelbrandt, Nathan Brubaker, Keith Lunden

Data leaks have always been a concern for organizations. The exposure of sensitive information can result in damage to reputation, legal penalties, loss of intellectual property, and even impact the privacy of employees and customers. However, there is little research about the challenges posed to industrial organizations when threat actors disclose sensitive details about their OT security, production, operations, or technology.

In 2021, Mandiant Threat Intelligence continued observing ransomware operators attempting to extort thousands of victims by disclosing terabytes of stolen information on shaming sites. This trend, which we refer to as "Multifaceted Extortion," impacted over 1,300 organizations from critical infrastructure and industrial production sectors in just one year.

To validate the extent to which multifaceted extortion leaks represent a risk to OT, Mandiant analyzed a semi-random selection of samples from industries that typically leverage OT systems for production. Using various technical and human resources, we downloaded and parsed through many terabytes of dump data and found a substantial amount of sensitive OT documentation. This included network and engineering diagrams, images of operator panels, information on third-party services, and more. We note that our analysis of each dump was limited due to the scale of our dataset and that a more targeted examination of a handful of dumps would probably uncover more documentation per organization.

Continue to the full article

A Scenario for Why Cyber Security and Evaluation Tool (CSET) is Important to Critical Infrastructure

Summertime is vacation time, and Scott and his young family are headed for the coast.

The family SUV is full of laughter and sunshine as Scott and his family of four (plus one on the way) are pointed toward the Atlantic Ocean. The hand shovels and plastic buckets are neatly stowed, and the cooler is packed with sandwiches, ginger ale, and mom's homemade fig newtons.

The morning traffic slows and merges as it approaches the intersection near the Chelsea Street Bridge, a scenic 450-foot vertical lift drawbridge, in northeast Boston. Wedged in among the trucks and commuters, Scott slowly works the family Ford closer and closer to the bridge, and closer and closer to the waters of Chelsea Creek. At last, Scott works into position, and is fully committed to the river crossing.

Scott has crossed the Chelsea Street Bridge hundreds of times and knows the drill. Most days he just cruises past the red-and-white safety drop-gates at the entrance and continues on his way. But Scott is soon to find out today will not be like most days.

Moments after rolling past the giant safety gates and onto the first third of the bridge, the gates drop behind him, the warning bells begin to sound, and the tell-tale whine of the bridge motors signal the center section of the bridge is about to go straight up.

Scott slams on the brakes as the cargo truck ahead stops short. He looks left and out his window

and sees the metal junction that marks the boundary between the bridge section and the ground section. Just then, then he hears a deep 'clunk' as the anchoring bolts disengage – signaling the final moment before the Chelsea Street Bridge separates.

An audible gasp from his wife in the passenger seat breaks Scott out of his trance, and he realizes he and his family have just one shot at escaping the unthinkable. Scott is too close to the truck ahead to freely get by on either side. And with the drop-gate behind and time running out, reverse is not an option.

Continue to the full article

The Belarus Cyber Attack – Addressing IT/OT Interdependence

By: Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

Ukrainian conflict puts critical infrastructure at risk

Belarussian "cyber activists" disrupted passenger rail traffic in the country by encrypting ticketing and other IT systems. The activists demanded that the government stop hosting Russian troops and demanded the release of 50 political prisoners before the attackers would relinquish control of the encrypted servers. The group threatened to extend their control into safety-critical rail switching systems if their demands were not met. In such an eventuality, the group said that their objective would be to shut down trains, especially those carrying Russian troops, not to threaten human lives.

What does this mean for the world?

Governments have already warned that national critical infrastructures are likely to be targets of cyberattacks, and this is doubly true in times of physical conflict. In addition, some governments have cautioned that targeting critical infrastructures with cyber-attacks may constitute acts of war. Cyber acts of war, however, will have to get in line behind physical acts of war if the Russia/Ukraine conflict escalates into a physical conflict where Ukraine, Ukrainian allies, and NATO are in effect at war with Russia and her allies.

Keeping the lights on

The attack on the Belarusian rail system is yet another example of an attack that cripples IT systems, and so brings about OT consequences, like the Colonial Pipeline attack, and the JBS meatpacking attack. In this case the rail system attack brought about confusion, delayed passenger trains and cancellations, all because of crippled ticketing systems. As a rule, such physical consequences are unacceptable to societies and their governments when those consequences impair critical national infrastructures.

Continue to the full article

The Benefits of Security Configuration Management for OT environments

By: Ben Jackman, CISSP – Tripwire

We all know it

OT organizations are struggling with legacy devices and a flood of vulnerabilities to ICS components. What's more, many industrial networks and servers were configured years ago - probably by someone with a degree in Chemical or Industrial Engineering degree - and most likely with out-of-the-box settings.

On one hand, we recognize that both scanning and patching vulnerabilities is not so simple in OT. But on the other hand, the OT security market continues to promote fear, uncertainty, and doubt - better known to marketers as FUD: *the attackers are already on your network, you need sophisticated threat intelligence feeds, and you better have the ghostbusters on speed dial for IR*. The security market continues to teeter back and forth between the spectrum of promoting prevention versus detection and response.

The truth is

The attack surface of your OT environment is actually more dependent on the security posture of traditional IT devices running on your industrial networks. Traditional IT vulnerabilities and misconfigurations are much easier targets for hackers - and these are the means the attacker will laterally (or vertically) move through your IT-DMZ-OT network chain.

Put another way, if an attacker is in a position on your industrial network to exploit an ICS component's vulnerability, then it's already game-over; they have elevated privileges and access to your engineering workstations, control database, etc. It would be much simpler for them to cause mayhem by deleting or modifying your process control algorithms and HMI diagrams than to exploit some peculiar ICS vulnerability.

Continue to the full article

Profitability in Peace: Protecting Nuclear ICS Vulnerabilities

By: Lindsey Warner, Consultant, Deloitte & Touche, LLP

Introduction:

ICS is a growing security industry that continues to evolve from cyber-attacks to causing physical damage with a click of a button. From anywhere in the world ICSs can be targeted and damaged in a matter of seconds by exploiting vulnerabilities. While threats and risks are not new, the scale in which an ICS outage can disrupt top targeted industries is a continuous learning curve. ICS attacks are significantly increasing, thus the business surrounding ICS challenges evolving technologies. ICS cyber-attacks are alarmingly rising due to a demand to profit from real world risk. These attacks are defining a new movement in securing ICS from outdated technologies into a new automated digital tool, which also changes the scope of incoming malicious activity. While the probability of modernization of Nuclear ICSs mitigates exposure to global and national vulnerabilities, new system operational challenges and clandestine operations, the long-term profitability in funding on a large scale today allows for a better protected tomorrow.

Nuclear ICS on a Global Front

The emergence of ICS as a key weakness in the global cyberwarfare race has intensified over the years to form one of the most dangerous frontline damaging attacks. The longstanding Israeli-Iran tête-à-tête, most notably the cyber-attack on Iran's Natanz plant and Israeli water treatment plant attacks, are another reminder of how quickly grids can be shut down. These strongly echo the Stuxnet stunt that demonstrated the full scale of how dangerous cyber-attacks can be on ICSs. These attacks can result in physical damage as well as business interruption which affects a globalized economy. Critical infrastructure is a major target for terrorist groups as well as government entities as it's hard to differentiate between espionage and malfunction. As nuclear plants are one of the most vulnerable infrastructures to protect, mostly due to outdated systems being converted to OT, malicious groups are constantly targeting these plants on a global front. Nuclear vulnerabilities extend further than just damaging property or potential loss of life, it can trigger a lack of credibility in deterrence or even provoke military response. Weapons systems are critically underdeveloped in most reported cyber vulnerabilities, leading to miscalculation and misunderstanding between nation states and their allies. Thirty countries have operational nuclear power, and approximately fifty are under construction. Nuclear vulnerabilities on a global front are a top priority for securing ICS, but especially for the United States as modernization becomes a primary focus.

Continue to the full article

Vulnerability Identification in Binary Files

By: Bryan Beckman, Senior Infrastructure Protection Idaho National Laboratory – Idaho Falls, ID USA National and Homeland Security, Critical Infrastructure Protection
bryan.beckman@inl.gov

Abstract

Software is regularly written for one purpose and reused for others. These often come in the form of pre-compiled libraries. This is certainly the case in ICS environments where updates are infrequent, and cost of downtime is high. Code reuse certainly has its benefits, including shortening the code development cycle, or if the library being used is open sourced, the benefit of having many eyes look at and analyze the code for bugs prior to use. Code reuse also has its drawbacks. For example, a code library may have been developed years ago and is still being used in a particular project, that library might no longer be supported and is simply used because it works. Additionally, other long forgotten code segments may find their way into a project as the project is edited by many other developers. The issue with these examples is that these code pieces may unknowingly bring vulnerabilities along with them. These vulnerabilities can, in turn, compromise the entire project. In this article, I will discuss the process that we at The Idaho National Laboratory have developed to identify any vulnerabilities and weaknesses that may exist in a pre-compiled test binary. Armed with this information, developers can patch and update their internal libraries. With this same process, IT professionals can scan binaries on their networks for vulnerabilities and request the vendor issue an update.

Introduction

This process makes use of a few tools developed by INL. These tools include @DisCo which disassembles and processes binary files for further analysis, as well as a script for extracting subgraphs from a much larger master graph. In this article, we will use a binary version of nmap[1] as the binary in question, as well as various versions of libssh2[2] as the potential vulnerable library we are concerned might be included in the nmap binary. The research and development of this process was completed as part of the Cyber Quality and Resilience Operations (Cyber QR Ops) project sponsored by the Department of Homeland Security (DHS), Science and Technology (S&T) Directorate.

Continue to the full article