ICS-CERT MONITOR

July, August, September 2013

NCCIC

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

CONTENTS

Contact Information

For any questions related to this report or to contact ICS-CERT:
Email: ics-cert@hq dhs gov
Toll Free: 1-877-776-7585

I Want To

- Report an ICS incident to ICS-CERT
- Report an ICS software vulnerability
- Get information about reporting

Downloading PGP/GPG Keys
http://ics-cert us-cert gov/sites/default/files/documents/ICS-CERT asc

Joining the Secure Portal

ICS-CERT encourages U S asset owners and operators to join the Control Systems compartment of the US-CERT secure portal Send your name, telephone contact number, email address, and company affiliation to ics-cert@hq dhs gov requesting consideration for portal access

ICS-CERT continuously strives to improve its products and services You can help by answering a short series of questions about this product at the following URL: https://forms us-cert gov/ncsd-feedback/

INCIDENT RESPONSE ACTIVITY

CRITICAL MANUFACTURING CYBER INCIDENT

ICS-CERT recently supported the incident response efforts for a critical manufacturing company. The company worked with both ICS-CERT and law enforcement officials to respond to intrusion activity and to mitigate risks to their networks and systems. ICS-CERT provided analytic support to the company including digital media analysis, onsite support, and an in-depth network assessment that included a Network Architecture Validation and Verification (NAVV).

After initial coordination discussions, the manufacturer sent copies of hard drives and virtual machines to ICS-CERT for digital media analysis. ICS-CERT conducted analysis and confirmed the presence of malware on several business systems, one of which contained an unpatched application. Company staff indicated that this particular system was likely the initial infection vector when a user opened a spear-phishing email while connected to it. It was believed that the attacker was then able to move laterally through the corporate network.

At that time, the extent of the compromise was unknown, and the manufacturer requested additional assistance onsite.

A team of ICS-CERT analysts worked onsite with company personnel to review their network diagrams and ran tools aimed at discovering additional indications of compromise and compromised hosts. The ICS-CERT onsite team objectives included:

- Access possible attack surfaces that might represent vulnerabilities from the corporate to SCADA environment;
- Provide additional context of threat actor techniques and tactics;
- Perform a CSET® assessment;
- Inspect and analyze available data from systems specifically identified as potentially infected (log files, memory dumps, and forensic images);
- Work with company representatives to acquire drive images and additional digital artifacts;
- Review access controls and network access rules for the company network architecture with focus on support connections to customer control systems networks;
- Assess data retention and recovery capabilities, antivirus tools, and technical support connections;
- Review network diagrams as well as data provided by the company including systems configuration of network security and network management devices; and
- Conduct an in-depth NAVV review.

The ICS-CERT team members and company representatives also conducted a physical tour of the primary facility to review the corporate network infrastructure, manufacturing facilities, and testing facilities. During the assessment, the ICS-CERT team and the company representatives discussed lessons learned during the incident response. The company used those recommendations to improve its cybersecurity architecture.

INTERNET CONNECTED CONTROL SYSTEMS

ICS-CERT continues to field reports of Internet-connected control systems from various researchers, including Bob Radvanovsky of Project SHINE, who leverage tools such as SHODAN to locate control systems devices or related SCADA products. ICS-CERT appreciates the efforts of these researchers to help improve the overall security of the community by reporting findings and raising awareness of the risks that exist when control components are not securely configured.

In a particular instance, a researcher reported an Internet facing control system to ICS-CERT that lacked password protection and was directly accessible.

ICS-CERT contacted the owner and confirmed that it was the facility's HVAC system. The business was using a third-party company to monitor the HVAC systems for the entire campus. The owner contacted the third-party company, which added credentials to secure the system. The other systems being monitored by the company were also checked and were all found to be secured. The system owner was responsive and had good knowledge of its system, which facilitated a quick remediation of the situation. From report of information to notification to securing of systems, the elapsed time was approximately 7 hours.

ICS-CERT recommends that control system owners and operators audit their control systems—whether they think their control systems are connected to the Internet—to discover and verify removal of any default administrator level user names and passwords. Because each control system installation is unique, owners and operators may need to contact their system vendor or integrator for assistance with locating and eliminating default accounts.

For more information visit http://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-343-01A and http://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-046-01A.

INCIDENT RESPONSE AND OUTREACH ACTIVITY

Recently, both ICS-CERT and the FBI have provided onsite and remote assistance to energy, manufacturing, and other critical infrastructure companies related to scans, probes, intrusions, and attempted access associated with an emerging threat actor. ICS-CERT provided details of these events through information products that were disseminated through the Control Systems Center on the US-CERT Secure Portal. The alerts provided information about:

- Attack methodology;
- Tactics, Techniques, and Procedures (TTPs);
- Lessons learned from incident response;
- Recommended practices and mitigation strategies for intrusion detection; and
- Improvement of existing cybersecurity.

In addition to incident response activities, ICS-CERT and the FBI, in coordination with the Department of Energy (DOE), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), Transportation Security Administration (TSA), the Oil and Natural Gas and Pipelines Sector Coordinating Council's Cyber Security Working Group, and other partners conducted a new series of "Action Campaign" classified briefings to provide further context of the threat and to highlight mitigation strategies. These briefings were similar to the outreach that ICS-CERT conducted in 2012 to highlight the cyber activity occurring at that time targeting Oil and Natural Gas (ONG) companies.

The briefing campaign began in June and is ongoing covering major markets across the US including Washington, DC; New York City, New York; Chicago, Illinois; Dallas, Texas; Denver, Colorado; San Francisco, California; San Diego, California; Seattle, Washington; Boston, Massachusetts; New Orleans, Lousiana; and numerous others via secure video teleconferences (SVTC).

To date, these action campaign classified briefings have reached nearly 700 private sector attendees.

Outreach activities in the form of risk and mitigation briefings play a key role in mitigating the overall risk to critical infrastructure. ICS-CERT will continue to conduct briefings as needed to provide asset owners with the most up-to-date information on emerging threats and security measures that can be deployed to help thwart cyber attacks and reduce risk.

If your critical infrastructure organization is interested in learning more about these threats and obtaining additional information, please contact ICS-CERT. Organizations who inquire and qualify may also receive membership into the Secure Portal where important and sensitive information is disseminated.

.

FREQUENTLY ASKED QUESTIONS

INCIDENT REPORTING

Some common questions that ICS-CERT receives from partners are "What is an incident?" and "When should we report to ICS-CERT?" In this edition, we tackle both questions to better define working with ICS-CERT for incident response.

What is an Incident?

A good but fairly general definition of an incident is the act of violating an explicit or implied security policy. This definition relies on the existence of a security policy that, while generally understood, varies among organizations.

For the federal government, an incident, defined by NIST Special Publication 800-61, is a violation or the imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

Examples of incidents are:

- Phishing or spear-phishing emails that are sent or received, or other attempts to lure users to open malicious attachments or click on links hosting malware;
- Denial-of-service attacks;
- Attempts to gain unauthorized access to a system or its data;
- Malware or other malicious code in the corporate or control environment; and
- Unauthorized changes to system hardware, firmware, or software characteristics.

US-CERT has defined federal incident reporting guidelines, including definitions and reporting timeframes for government users. More information can be found at http://www.us-cert.gov/government-users/reporting-requirements.

When to report to ICS-CERT?

We encourage organizations to report any activities that they think meet the criteria for an incident. ICS-CERT policy is to keep confidential any reported information specific to your organization or activity. Organizations can also leverage the Protective Critical Infrastructure Information (PCII) program to further protect and safeguard their information.

Generally speaking, ICS-CERT is best positioned to assist organizations with threats that are targeted in nature. These types of threats typically involve

- Well-crafted spear-phishing emails;
- Unusual or destructive malware; and
- Anything anomalous occurring or found in the control environment.

In addition, any denial of service or scanning of control systems assets should also be reported for tracking and correlation.

If an organization detects malicious activity but is unsure if they should be concerned, ICS-CERT recommends reporting the incident. In those cases, organizations can leverage ICS-CERT as a barometer to quickly evaluate, through a few questions and some quick analysis, whether the activity is targeted or severe in nature or is general nontargeted activity.

Organizations can report to ICS-CERT by emailing ics-cert@hq.dhs.gov or calling 877-776-7585. Organizations can download our PGP key at http://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT.asc

For more tips on improving your own incident handling and detection, please visit http://ics-cert.us-cert.gov/sites/default/files/Incident_Handling_Brochure_Nov_2010.pdf.

SITUATIONAL AWARENESS

APPLICATION WHITELISTING IN AN ICS ENVIRONMENT (PART 1 OF 2)

This is the first in a two-part series. Part 2, "Challenges of Application Whitelisting," will appear in the next edition of the Monitor.

BENEFITS AND LIMITATIONS OF APPLICATION WHITELISTING

WHAT IS APPLICATION WHITELISTING?

Application whitelisting (AWL) is a security technology that allows only authorized programs to run, while all unauthorized programs are blocked from running by default. AWL is implemented by creating and maintaining a list of approved or "whitelisted" applications and is enforced through a number of potential rule mechanisms that include file hashes (e.g., SHA1), certificates, trusted paths, and file names. When implementing AWL, it is important to consider and understand the tradeoffs between each of these rule mechanisms. Once the AWL policy is defined, most AWL products employ a software agent that is installed locally on each endpoint to enforce the specific policy. When the endpoint is secured with the agent, the agent will check each application that attempts to execute against the locally stored approved list of applications and then will either allow or block its execution. This is often referred to as secure-mode.

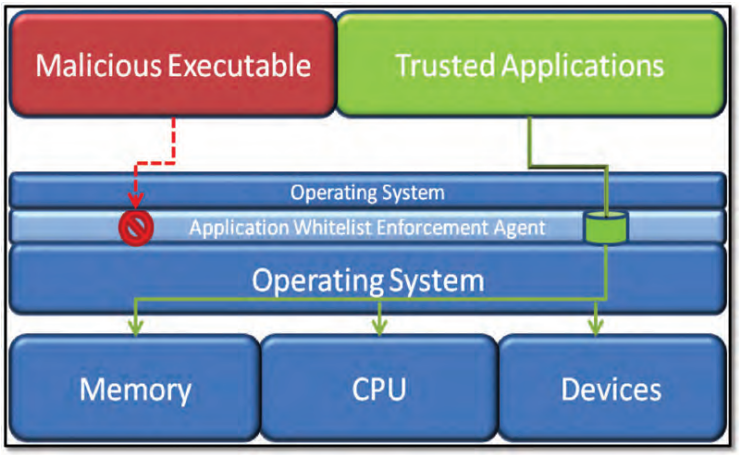


Figure 1. Application whitelisting endpoint secure-mode functionality. This figure shows how trusted applications are allowed to execute (green) while nonapproved (not whitelisted) applications such as malicious files are blocked (red).

The following sections provide some information about cyber attack methodology, which is useful in understanding AWL benefits and limitations. As will be explained, AWL offers solid protection against malicious executable attacks, but not against most exploitation attacks.

MALICIOUS EXECUTABLE ATTACKS

Malicious executables are programs resident on the target system whose primary purpose is to perform something harmful to a system. A file such as this can find its way onto a system in a variety of manners. Some of the more common ways are through Web downloads, email, file sharing, digital storage media. Memory resident exploits will also drop such a file as a second stage attack to maintain persistence or install additional toolkits beyond the capability of the original exploit payload.

The traditional method of protecting against this type of attack has been a combination of antivirus software and least privileges for users and applications.

EXPLOITATION ATTACKS

This set of attacks is related to software vulnerabilities. Attackers both with and without the help of system users leverage these vulnerabilities to gain control of target machines. These exploitation methods include attacks such as remote exploitation, client-side attacks, and file format vulnerabilities.

Remote Exploitation Attacks– Exploits that target vulnerable services that process incoming connections. Some examples of potentially vulnerable services include FTP, Telnet, SSH, and HTTP. This type of attack is achieved by sending malicious data to a vulnerable service in order to gain full control of the system without any user interaction.

Client-Side Attacks– Exploits that target vulnerabilities in applications that could potentially interact with a malicious server. A typical example of this type of attack is a threat that exploits a vulnerability in a user's Internet browser. This requires a user to visit the malicious site that in turn sends malicious data to exercise control of the system.

File Format Vulnerabilities– Exploits that target vulnerabilities in applications that interact with a malicious file to process harmful data. Examples of potentially vulnerable applications include Microsoft Word and Adobe Acrobat Reader. When the application attempts to process the malicious file, an attacker takes control of the system.

In order for exploitation attacks to be successful, the target application must contain a vulnerability that allows arbitrary code execution or corruption of data. For information on vulnerabilities in ICS, please refer to the DHS Common Cybersecurity Vulnerabilities in Industrial Control Systems Report.[1]

BENEFITS OF APPLICATION WHITELISTING

The primary benefit of AWL is the ability to inhibit the establishment of attacker persistence mechanisms on a system. This means that even if an attack succeeds by exploiting a software vulnerability, an attacker will have increased difficulty executing nonmemory-based additional malware on the system. AWL does this by allowing only authorized executables to run and blocking all unauthorized executables. This provides an advantage over antivirus technologies that use signature-based or "blacklist" detection techniques. The whitelisting approach is more effective in protecting against newer malicious executables that may go unnoticed by antivirus. This is made possible because the "default deny" approach is more strict and effective than a traditional "blacklist" approach used by antivirus programs. AWL solutions effectively block execution-based attacks (malicious executables) from running. These are attacks using machine native code (i.e., binary code) that is directly executed by an operating system. This is in contrast to interpreted languages that use an intermediary executable to translate the program into native instructions such as a Java virtual machine or the .NET Common Language Runtime framework.

AWL solutions are also designed to provide system administrators with a robust means by which to audit and monitor all executables on all endpoints on the network through a centralized management console. This allows for improved change management and creation of timelines that can be used to detect, confirm, and respond to an attack even if run in monitor-only mode. Monitor-only mode differs from secure-mode in that it only records installation and execution events but takes no action to block the execution of programs on the endpoint.

Finally, AWL can provide a mechanism to improve regulatory compliance. For example, AWL maps directly to the Critical Infrastructure Protection (CIP) Cyber Security Standards (NERC CIP Standards 002-009[2]) that apply to the bulk power system. Specifically, requirements to which AWL can apply are:

- CIP-003-4 R6 Change Control and Configuration of Management,
- CIP-005-4a R1 Electronic Security Perimeter,
- CIP-007-4 R2 Port and Services, and
- CIP-007-4 R4 Malicious Software Prevention.

LIMITATIONS OF APPLICATION WHITELISTING

AWL does have limitations and should be considered as one layer in a defense-in-depth[3] cybersecurity strategy rather than a sole solution. Probably the most notable limitation is that AWL does not protect systems from exploitation attacks that target vulnerabilities in trusted applications. These applications are on the AWL-approved list and are allowed to execute. Examples of exploitation attacks include SQL injection, cross-site scripting (XSS), and memory corruption attacks such as buffer overflows. However, implementation of memory protection technologies included in many AWL solutions does provide a greater level of protection against memory-based attacks. AWL can be further limited by the inability to block programs running in higher level execution environments. Examples of such environments are Java Runtime, .NET Framework, and scripting languages. These programs run at a higher level in the operating system and provide a different context for execution. Instead of running a traditional binary malware artifact, an attacker can write a program for this context and place this on the system. If this environment is whitelisted and allowed, code execution is possible. Even with these limitations, it is important to understand that AWL can limit the scope of these types of attacks, because it will make it more difficult for an attacker to establish a persistent presence by stopping execution of a dropped malicious file on the vulnerable systems. It may also force attackers to change tactics and make them easier to discover. Dropped malicious files are important to attackers because they provide additional capability to an attacker beyond the exploit's original payload.

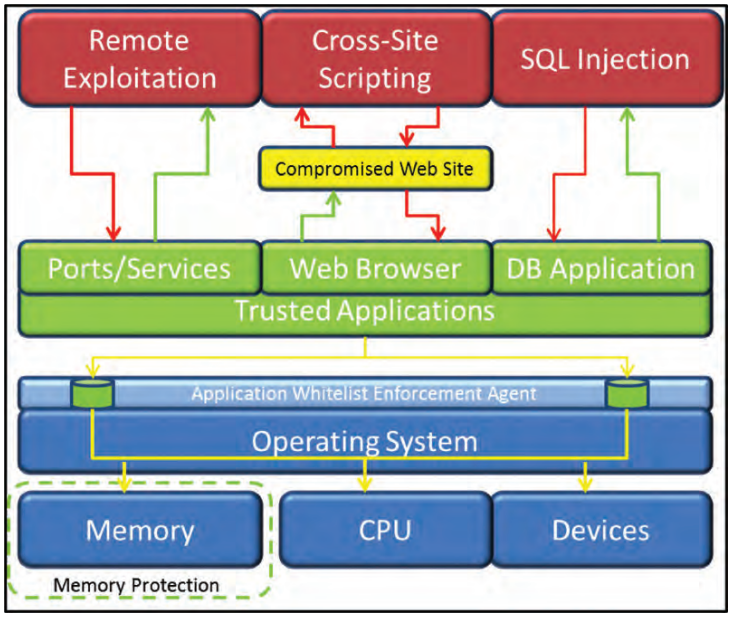


Figure 2. Application whitelisting endpoint secure-mode functionality (Remote Exploitation). This figure shows that an attacker can still leverage trusted applications for attacks even with the protection whitelisting technology provides.

References

1 DHS, Common Cybersecurity Vulnerabilities in Industrial Control Systems, http://ics-cert us-cert gov/sites/default/files/documents/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010 pdf May 2011, Site last accessed January 2013

2 NERC Reliability Standards, http://www nerc com/page php?cid=2%7C20, January 2012, Site last accessed August 28, 2013

3 DHS, Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies, http://ics-cert us-cert gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09 pdf, October 2009, Site last accessed January 2013

CYBER RISKS ASSOCIATED WITH MAS RADIOS

Multiple Address System (MAS) radio is an extremely popular communication setup for SCADA systems, given its low cost, flexibility, and ease of use. A typical setup includes a master radio and several remote units. MAS has a point-to-multipoint architecture (either one or two-way) and generally operates in the 900-MHz frequency band to communicate with remote terminal units (RTUs).

Depending on the geographic topology, the transmitter power and the type of antenna, a radio system can provide coverage over a 20 to 30-mile radius. However, the area covered by a MAS radio varies depending on which spread-spectrum frequencies (licensed or unlicensed bands) are used. Traditionally, licensed radios provided the added benefit of protection from interference (not so with unlicensed spectrum radio). However, an increase in the

number of FCC licenses issued has led to oversaturation in some spectrum ranges, minimizing that advantage. In addition, these radio systems, while relatively inexpensive, are limited to line-of-sight communication.

In its simplest form, the central SCADA system is usually equipped with an omnidirectional antenna, while the remote stations have directional (yagi) antennas oriented toward the main system. The Master and RTU radios (transceivers) are keyed to a specific frequency. (More complex systems might use multiple master stations operating on different frequencies.)

MAS radios, especially those employed as wireless communication links, have a number of security vulnerabilities and face spoofing, denial of service, and man-in-the-middle attacks. In 2009, a presenter at DEFCON17 illustrated his success hacking a MAS radio using an antenna small enough to fit in his compact car. While not the most sophisticated setup, by keying to the input frequency, the presenter was able to instigate communication failures through a denial-of-service attack. This example highlights the lack of security common to MAS radios. Still, while these systems are often insecure, they are rarely responsible for critical communication functions and are more often used to provide measurement data to the control system.

In December 2012, Bradley Reeves and Thomas Morris published an article, "Analysis and Mitigation of Vulnerabilities in Short-range Wireless Communication Systems for Industrial Control Systems," which included a number of recommendations to improve the security of wireless technologies including:

- Manage bandwidth usage: Not only will this improve the reliability of wireless systems, but it will also limit the effectiveness of denial-of-service attacks. Managing bandwidth becomes more difficult when working with unlicensed frequencies or when more than one organization is operating within radio range of each other.
- Employ directional antennas whenever possible: While directional antennas can increase security, they come with the tradeoff of limiting their directionality and ability to send and receive messages. In some setups, such as ZigBee or WirelessHART, the loss of a central node impedes the organization more than poor wireless security. Border nodes, however, can be upgraded to directional antennas for a one-time cost and have the added benefit of increased system performance.
- Limit the potential attack surface by placing the wireless devices as close to ground level as possible: This is a relatively inexpensive security precaution provided it is developed in the design phase.
- Organizations should not rely on the short-range nature of these protocols for security: Groups should adopt additional protocol-specific security measures, including strong password requirements.
- Organizations should conduct routine risk assessments in order to identify the critical information being transmitted on their networks: Critical data, such as those responsible for transmitting control processes, should be identified and treated accordingly.

Wireless networks enhance the monitoring and control capabilities of MAS radio, but also introduce vulnerabilities. Those risks should be recognized and mitigated by the organizations using those systems.

We Want To Hear From You

A key aspect of our mission is providing relevant and timely cybersecurity information products and services to industrial control system (ICS) stakeholders. As we develop and prepare new products, we need and want your input, both good and bad. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Your feedback is welcomed, so we can work together to meet the security challenges facing the ICS community.

If you want to see an important or pertinent topic addressed in this forum, please send your suggestions to: ics-cert@hq.dhs.gov.

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

RECENT PRODUCT RELEASES

ALERTS

ICS-ALERT-13-164-01 Medical Devices Hard-Coded Passwords, 6/13/2013

ADVISORIES

ICSA-13-231-01B Sixnet Universal Protocol Undocumented Function Codes, 9/17/2013

ICSA-13-231-01A Sixnet Universal Protocol Undocumented Function Codes, 8/26/2013

ICSA-13-234-01 Schneider Electric Trio J-Series Radio Encryption, 8/22/2013

ICSA-13-234-02 Top Server OPC Improper Input Validation Vulnerability, 8/22/2013

ICSA-13-233-01 Siemens COMOS Privilege Escalation Vulnerability, 8/21/2013

ICSA-13-226-01 Kepware Technologies Improper Input Validation Vulnerability, 8/14/2013

ICSA-13-225-01 Advantech WebAccess Cross-Site Scripting, 8/13/2013

ICSA-13-225-02 OSIsoft Multiple Vulnerabilities, 8/13/2013

ICSA-12-228-01A Tridium Niagara Multiple Vulnerabilities, 8/12/2013

ICSA-13-219-01 Schweitzer Engineering Laboratories Improper Input Validation, 8/7/2013

ICSA-13-217-01 MOXA Weak Entropy in DSA Keys Vulnerability, 8/5/2013

ICSA-13-217-02 Schneider Electric Vijeo Citect, CitectSCADA, PowerLogic SCADA Vulnerability, 8/5/2013

ICSA-13-213-01 Siemens Scalance W-7xx Product Family Multiple Vulnerabilities, 8/1/2013

ICSA-13-213-02 Siemens WinCC TIA Portal Multiple Vulnerabilities, 8/1/2013

ICSA-13-213-03 IOServer Master Station Improper Input Validation, 8/1/2013

ICSA-13-170-01 GE Proficy HMI/SCADA CIMPLICITY WebView Improper Input Validation, 7/30/2013

ICSA-13-189-01 QNX Multiple Vulnerabilities, 7/8/2013

ICSA-13-189-02 Triangle Research Nano 10 PLC Denial of Service, 7/8/2013

ICSA-13-184-01 Alstom Grid S1 Agile Improper Authorization, 7/3/2013

ICSA-13-184-02 Monroe Electronics DASDEC Compromised Root SSH Key, 7/3/2013

ICSA-13-169-01 Siemens Scalance X200 IRT Multiple Vulnerabilities, 6/18/2013

ICSA-13-169-02 Siemens WinCC 7.2 Multiple Vulnerabilities, 6/18/2013

ICSA-13-169-03 Siemens COMOS Permissions, Privileges, and Access Controls, 6/18/2013

ICSA-13-161-01 IOServer DNP3 Improper Input Validation, 6/10/2013

ICSA-12-018-01A Schneider Electric Quantum Ethernet Module Hard-Coded Credentials, 6/4/2013

ICSA-13-077-01B Schneider Electric PLCs Multiple Vulnerabilities, 6/4/2013

OTHER

April/May/June 2013–ICS-CERT Monitor

Follow ICS-CERT on Twitter: @icscert

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

Hackers can now target light bulbs, security researcher warns
2013-08-14

In the modern world, everything is online -- and unsafe. That's the message from researcher Nitesh Dhanjani, who discovered a vulnerability in Philips new line of smartphone-controlled lightbulbs that would allow a hacker to remotely turn them on and off, an action that could have major consequences in hospitals and other public venues, he said.

http://www foxnews.com/tech/2013/08/14/hackers-target-light-bulbs/?test=latestnews

New York Times website goes down
2013-08-14

The New York Times website is down and it's unclear what caused the outage. The company's newspaper and corporate sites also appeared to be effected. Emails sent to New York Times email addresses were returned as undeliverable.
http://www foxnews.com/us/2013/08/14/new-york-times-website-goes-down/

Smart toilet security flaw could result in nasty surprise
2013-08-05

It's probably fair to say that the worst thing that can happen while you're on the toilet is discovering there's no paper in the holder at the very moment you go to reach for it. Owners of a high-tech Satis toilet from LIXIL now have something else to worry about. According to software security firm Trustwave, the super-advanced smart toilet can be hacked. That's right, malicious attackers could take control of your cutting-edge commode and get it to do just about anything, and possibly at the most inconvenient of moments. According to Trustwave's Daniel Crowley, at the center of the security vulnerability is the accompanying My Satis Android app, which communicates with the toilet using Bluetooth, enabling the user to operate its various functions using a handset or tablet. "The My Satis Android application has a hard-coded Bluetooth PIN of 0000," Crowley explained. "As such, any person using the application can control any Satis toilet."

http://www foxnews.com/tech/2013/08/05/smart-toilet-security-flaw/

The five scariest hacks we saw last week
2013-08-05

If something can connect to a network, it can be hacked. Computers and phones are still popular targets, but increasingly so are cars, home security systems, TVs and even oil refineries. That was the message at this year's Black Hat and DefCon computer security conferences, which took place last week in Las Vegas. The annual conferences draw a mix of computer researchers and hackers who present the latest bugs and vulnerabilities they've discovered. It's a combination of public service, business and sport. These are some of the more popular targets covered at this year's conferences. By drawing attention to them, the "white-hat" hackers hope to encourage greater security from the various manufacturers and industries, and more vigilance from consumers. Typically, the presenters inform manufacturers of bugs ahead of their talks so the companies can fix the issues before they are exploited by criminals.

http://www.cnn.com/2013/08/05/tech/mobile/five-hacks/index.html?hpt=hp_bn5

Hackers plan to offer blueprint for taking over Prius, Escape
2013-07-30

Two well-known computer software hackers plan to publicly release this week a veritable how-to guide for driving two widely owned automobiles haywire. According to Reuters, Charlie Miller and Chris Valasek will release the findings -- as well as related software -- at the Def Con hacking convention in Las Vegas, showing how to manipulate a Toyota Prius and Ford Escape. The research, conducted with the aid of a grant from the U.S. government, can alternately force a Prius to brake at 80 mph, veer quickly and dramatically, or accelerate, all without the driver's prompting. The two hackers have also reportedly figured out a way to disable a Ford Escape's brakes while the vehicle is traveling at "very low speeds," no matter how hard the driver attempts to stop. In both cases, the would-be hacker would have to be inside the car in order to tamper with its computer, according to Reuters.
Hackers plan to offer blueprint for taking over Prius, Escape

http://www foxnews.com/tech/2013/07/28/hackers-plan-to-offer-blueprint-for-taking-over-prius-escape/#ixzz2ap8DMhTn

Pipelines to Pacemakers: Defending Our Medical Devices With Help From the Energy Sector
2013-07-29

The FDA dropped a bombshell on the health care industry last month, and companies are missing the quickest and easiest way to respond. The FDA's latest recommendation (June 13, 2013) that "medical device manufacturers and health care facilities take steps... to reduce the risk of failure due to cyberattack," has the opportunity to cause a wave of waste and expensive false senses of security unless approached with a proven risk process for securing these types of devices.

Unlike the medical industry, the energy sector -- from pipelines to oil rigs to power grids -- has long been at risk due to the relatively

small industrial control systems, or ICS, that perform much of their automated decision making. While the form and function of a pacemaker and an oil pipeline are very different, the approach to securing them can be highly symbiotic. These third-party ICS are implanted into the body of an oil rig or pipeline, and then left to open and close valves, start and stop pumps, and other low level but crucial tasks. In the energy space, a false command to a valve or a pump can cause blackouts, oil slicks, or toxic clouds.

http://www huffingtonpost.com/tom-patterson/pipelines-to-pacemakers_b_3671229.html

Google Glass Hacked With QR Code Photobombs
2013-07-17

Researchers at the security firm Lookout Mobile say they developed an attack last spring that could compromise Google's device when the user merely took a photo that captured a malicious QR code, the square graphic labels often used to link smartphone users to websites and by Google Glass to set up the headset's Wifi connections. Lookout's researchers, who reported the bug to Google and have already helped the company issue a fix for the flaw, found that they could craft malformed QR codes that when photographed crashed Glass or connected the headset to a rogue Wifi hotspot capable of stripping away the encryption on the device's communications or directing it to a malicious website designed to take full control of the device.

http://www forbes.com/sites/andygreenberg/2013/07/17/google-glass-hacked-with-qr-code-photobombs/

Nations Buying as Hackers Sell Flaws in Computer Code
2013-07-13

The hackers, Luigi Auriemma, 32, and Donato Ferrante, 28, sell technical details of such vulnerabilities to countries that want to break into the computer systems of foreign adversaries. The two will not reveal the clients of their company, ReVuln, but big buyers of services like theirs include the National Security Agency — which seeks the flaws for America's growing arsenal of cyberweapons — and American adversaries like the Revolutionary Guards of Iran.

http://www nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws html

Protecting water and wastewater facilities from cyberattack
2013-07-10

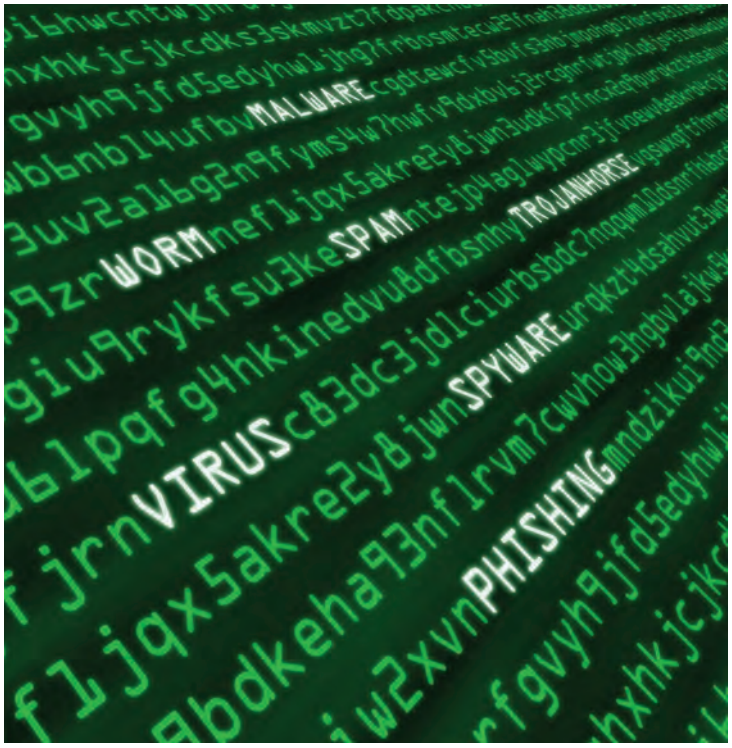
"If you aren't scared yet, you haven't been paying attention." So goes the aphorism for modern times, and it applies equally well to industrial cybersecurity. Conclusive proof is hard to come by, but consider the supporting evidence: U.S. presidential executive orders, vulnerabilities markets for ICS, U.S. Secretary of Defense warnings of a "cyber Pearl Harbor," extremely low patch uptake for ICS/IT automation components, vast and Security with Lock, varied ICS CERT warnings, Internet census reports of huge populations of exposed ICS systems. Before Stuxnet, stories like this just didn't get any attention if they were even published. All industries are affected. Water and wastewater environments are no different, and in fact are particularly attractive to threat actors not only because they are the foundation of advanced societies, but because they are easy targets.

http://automation.isa.org/2013/07/protecting-water-and-wastewater-facilities-from-cyberattack/

"Ultimately, none were successful"
2013-07-08

The spring edition of the ICS-CERT Monthly Monitor's lead story is "Brute Force Attacks On Internet Facing Control Systems." It got picked up by a large number of the mainstream press including the Wall Street Journal. Author Rachel King points out that according to ICS-CERT, "These attempted attacks originated from 49 IP addresses but ultimately, none were successful".

http://www.digitalbond.com/blog/2013/07/08/ultimately-none-were-successful/



OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS - Continued

We interrupt this program to warn the Emergency Alert System is hackable
2013-07-08

The US Emergency Alert System, which interrupts live TV and radio broadcasts with information about national emergencies in progress, is vulnerable to attacks that allow hackers to remotely disseminate bogus reports and tamper with gear, security researchers warned.

http://arstechnica.com/security/2013/07/we-interrupt-this-program-to-warn-the-emergency-alert-system-is-hackable/

Opera Software Hit by 'Infrastructure Attack'; Malware Signed with Stolen Cert
2013-06-26

Norwegian browser maker Opera Software has confirmed that a targeted internal network infrastructure attack led to the theft of a code signing certificate that was used to sign malware.

http://www.securityweek.com/opera-software-hit-infrastructure-attack-malware-signed-stolen-cert

Remote-Control Model Plane Attack 'Foiled'
2013-06-26

Two aeronautics students planned to use remote-controlled model planes packed with explosives to carry out terrorist attacks in Germany, according to prosecutors.

http://uk news.yahoo.com/remote-control-model-plane-attack-foiled-205754696 html#qQSPlKr

A major cyber threat to critical infrastructures is from ... the electric utilities
2013-06-04

Critical infrastructures include water, oil/gas, pipelines, chemicals, manufacturing, telecommunications, transportation, etc. Their continued operation requires the electric utility industry to be available. However, the electric utility industry is also a cyber threat to all of those end-users. That threat is Aurora. As a result, Aurora throws the traditional concept of interdependencies on its ear.

http://community.controlglobal.com/content/major-cyber-threat-critical-infrastructures-electric-utilities

DOCUMENT FAQ

What is the publication schedule for this digest?

ICS-CERT publishes the ICS-CERT Monitor when an adequate amount of pertinent information has been collected.

ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets. The public can view this document on the ICS-CERT Web page at: http://www.us-cert.gov/control_systems/ics-cert/.

Please direct all questions or comments about the content, or suggestions for future content, to ICS-CERT at: ics-cert@hq.dhs.gov.

UPCOMING EVENTS 2013

November

Industrial Control Systems Cybersecurity (301) Training (5 days)
North American Partners
CLOSED
November 4–8, 2013
Idaho Falls, Idaho

December

Industrial Control Systems Cybersecurity (301) Training (5 days)
North American Partners
CLOSED
December 2–6, 2013
Idaho Falls, Idaho

January 2014

Industrial Control Systems Cybersecurity (301) Training (5 days)
North American Partners

January 13-17, 2014
Idaho Falls, ID
Course Description and Registration

COORDINATED VULNERABILITY DISCLOSURE

ICS-CERT actively encourages researchers and ICS vendors to use a coordinated vulnerability disclosure process when possible. Ideally, this coordinated disclosure process allows time for a vendor to develop and release patches, and for users to test and deploy patches prior to public vulnerability disclosure. While this process is not always followed for a variety of reasons, ICS-CERT continues to promote this as a desirable goal.

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US-CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact ICS-CERT at
ics-cert@hq.dhs.gov or toll free at 1-877-776-7585.

RESEARCHERS Assisting ICS-CERT with products that were published JULY/AUGUST/SEPTEMBER.

ICS-CERT appreciates having worked with the following researchers:

- Independent researcher Mehdi Sabraoui, ICSA-13-231-01A, Sixnet Universal Protocol Undocumented Function Codes, 8/26/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-234-02, Top Server OPC Improper Input Validation Vulnerability, 8/22/2013
- Independent researcher Mehdi Sabraoui, ICSA-13-231-01, Sixnet Universal Protocol Undocumented Function Codes, 8/19/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-226-01, Kepware Technologies Improper Input Validation Vulnerability, 8/14/2013
- Independent researcher Sanadi Antu, ICSA-13-225-01, Advantech WebAccess Cross-Site Scripting, 8/13/2013
- Independent security researchers Billy Rios and Terry McCorkle, ICSA-12-228-01A, Tridium Niagara Multiple Vulnerabilities, 8/12/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-219-01, Schweitzer Engineering Laboratories Improper Input Validation, 8/7/2013

COORDINATED VULNERABILITY DISCLOSURE - Continued

- Researcher Nadia Heninger of the University of California, San Diego, and researchers Zakir Durumeric, Eric Wustrow, and J. Alex Halderman of the University of Michigan, ICSA-13-217-01, MOXA Weak Entropy in DSA Keys Vulnerability, 8/5/2013
- Researchers Timur Yunusov and Sergey Bobrov of Positive Technologies, ICSA-13-213-02, Siemens WinCC TIA Portal Multiple Vulnerabilities, 8/1/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-213-03, IOServer Master Station Improper Input Validation, 8/1/2013
- Independent researchers ZombiE and amisto0x07, ICSA-13-170-01, GE Proficy HMI/SCADA CIMPLICITY WebView Improper Input Validation, 7/30/2013
- Independent researcher Luigi Auriemma, ICSA-13-189-01, QNX Multiple Vulnerabilities, 7/8/2013
- Researcher Jon Christmas of Solera Networks, ICSA-13-189-02, Triangle Research Nano 10 PLC Denial of Service, 7/8/2013
- Mike Davis, a researcher with IOActive, ICSA-13-184-02, Monroe Electronics DASDEC Compromised Root SSH Key, 7/3/2013
- Researchers Alexander Tlyapov, Sergey Gordeychik, and Timur Yunusov of Positive Technologies, ICSA-13-169-02, Siemens WinCC 7.2 Multiple Vulnerabilities, 6/18/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-161-01, IOServer DNP3 Improper Input Validation, 6/10/2013
- Independent security researcher Rubén Santamarta, ICSA-12-018-01A, Schneider Electric Quantum Ethernet Module Hard-Coded Credentials, 6/4/2013
- Independent researcher Arthur Gervais, ICSA-13-077-01B Schneider Electric PLCs Multiple Vulnerabilities, 6/4/2013

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT IN 2013

ICS-CERT appreciates the following researchers who continue to work with us to resolve exploits:

Aaron Patterson
Aaron Portnoy
Alexey Osipov
Andrew Brooks
Anton Popov
Artem Chaykin
Arthur Gervais
Billy Rios
Bob Radvanovsky
Brendan Harris
Carlos Mario Penagos Hollmann
Carsten Eiram
Cesar Cerrudo
Christopher Scheuring
Christopher Sistrunk
Dale Peterson
Dillion Beresford
Eric Wustrow
Gleb Gritsai
Hisashi Kojima
Ilya Karpov
J. Alex Halderman
Joel Langill
John Adam Crain
Jon Christmas
Juan Vasquez
Jürgen Bilberger
Kuang-Chun Hung (ICST)
Lucas Apa
Luigi Auriemma
Mashahiro Nakada
Michael Toecker
Nadia Heninger
Neil Smith
Nin3
Postive Technologies Security
Reid Wightman
Roman Ilin
Rubén Santamarta
Ryan Green
Sergey Bobrov
Sergey Gordeychick
Shawn Merdinger
Terry McCorkle
Timur Yunusov
Zakir Durumeric