ICS-CERT MONTHLY MONITOR

JUNE 2011

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

MONTHLY CYBER TIP

Patch Management

ICS-CERT recommends that owners establish policies for maintaining control systems software configurations with the most current updates. This includes monitoring vendor websites for available updates and ensuring that critical updates are tested for compatibility and applied as soon as possible. Cybersecurity experts recommend that users install and test all patches in a "sand box" (test) environment prior to installing them on a live control system.

Contact Information

For any questions related to this report or to contact ICS-CERT:

E-mail: ics-cert@dhs.gov

Toll Free: 1-877-776-7585

For Control Systems Security Program Information and Incident Reporting:

http://www.ics-cert.org

What is ICS-CERT?

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus to:

- Conduct vulnerability and malware analysis
- Provide onsite support for incident response and forensic analysis
- Provide situational awareness in the form of actionable intelligence
- Coordinate the responsible disclosure of vulnerabilities/mitigations
- Share and coordinate vulnerability information and threat analysis through information products and alerts.

The "ICS-CERT Monthly Monitor" offers a means of promoting preparedness, information sharing, and collaboration with the 18 critical infrastructure and key resource (CIKR) sectors. ICS-CERT accomplishes this on a day-to-day basis through sector briefings, meetings, conferences, and information product releases.

This publication highlights recent activities and information products affecting industrial control systems (ICSs) and provides a look ahead at upcoming ICS-related events.

VULNERABILITY DISCLOSURE

ICS-CERT works closely with industry, academia, private researchers, and law enforcement to respond to and resolve cybersecurity incidents that affect industrial control systems (ICSs). These incidents often provide lessons learned that apply to the overall critical infrastructure ICS community. This month's Monthly Monitor highlights recent events associated with ICS vulnerability disclosure.

Vulnerability Disclosure Is a Dynamic Process

ICS-CERT is continuously engaged in coordinating disclosures of vulnerabilities with private researchers and vendors, with the number of product vulnerabilities reported to ICS-CERT increasing at a significant rate. ICS-CERT expects this trend will continue into the foreseeable future. To address these vulnerabilities, ICS-CERT has formulated a vulnerability disclosure policy, available at http://www.us-cert.gov/control_systems/ics-cert/disclosure.html, which ICS-CERT encourages all vendors, researchers, and asset owners download and review. This policy defines in general terms how ICS-CERT processes vulnerability disclosure information in the ICS space. This policy statement is not a detailed description of the actual processes and procedures ICS-CERT executes when coordinating vulnerability information releases with researchers and vendors. This process remains dynamic and unique to each disclosure case. To help you understand this process, we are providing a high-level explanation of the coordination that ICS-CERT attempts to facilitate for all types of disclosures.

ICS-CERT Vulnerability Categorization

ICS-CERT categorizes vulnerability disclosures two ways:

1. Unanticipated Disclosure—This is when a researcher publicly releases information on vulnerabilities, exploits, or both, without prior coordination with the vendor or ICS-CERT. In these situations, the critical need is to notify those whose systems may be affected by the vulnerabilities of the publicly available information as well as any possible mitigations that may be available.

(continued on page 2)

ANNOUNCEMENTS

ICS-CERT Releases Report on "Common Cybersecurity Vulnerabilities in Industrial Control Systems"

In 2009, a report titled "Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments" compiled common vulnerabilities identified during 15 security assessments of new ICS products and production ICS installations from 2004 through 2008. Three additional ICS product assessments were performed in 2009 and 2010. This updated report has been developed to proactively create greater awareness within the ICS community. The common vulnerabilities correlated and compiled in this report represent general knowledge and trends gained from actual DHS CSSP assessments and ICS-CERT activities, and consist of three major types. These are:

1. Assessments of ICS products
2. Published products derived from ICS-CERT incident response operations
3. Self-assessment feedback from asset owners using the Cyber Security Evaluation tool (CSET).

To download this report, visit the CSSP web page (Information Products) at:

http://www.us-cert.gov/control_systems/pdf/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf.

VULNERABILITY DISCLOSURE

(from page 1)

2. Coordinated Disclosure—This is when a researcher brings the vulnerability to the attention of ICS-CERT allowing ICS-CERT to coordinate and validate the information exchange between the researcher and vendor. The researcher does not publicly release vulnerability details or potential exploits. Vulnerability details are released by ICS-CERT or the vendor in a staged manner to provide time for the vendor to release a validated patch/update and for users to obtain and install the patch/update.

Depending on the category of vulnerability disclosure, ICS-CERT follows one of the two general processes outlined below.

Unanticipated Vulnerability Disclosure Process

1. Because the researcher has already published an exploit for the reported vulnerability, the unanticipated disclosure process requires rapid, close coordination with the vendor (and possibly the researcher) to publicize useful mitigation strategies.
2. In these situations, ICS-CERT immediately releases an alert (ICS-ALERT-YY-DDD-SS) on the ICS-CERT public web page notifying critical infrastructure and key resources (CIKR) stakeholders of the potential threat. Occasionally, ICS-CERT will release an alert only to the US-CERT secure portal library when there is a need to limit the initial distribution to the vetted membership – primarily CIKR asset owners, federal, state, local, and tribal agencies.
3. Recognizing that CIKR asset owners and operators need more information on both the threat and possible mitigation strategies to protect their control systems from the now public vulnerability information or exploit, ICS-CERT usually releases a follow-up advisory as soon as possible after the initial alert, containing additional mitigation information if it exists.
4. The advisory includes additional details on vulnerability characterization and exploitability as well as specific mitigation strategies for users. ICS-CERT provides updates to advisories as needed.

Coordinated Vulnerability Disclosure Process

1. In these situations, because vulnerability details or exploits are not publicly released, ICS-CERT coordinates with the researcher to get the pertinent information to the vendor. ICS-CERT then works with the vendor to confirm the vulnerability and to validate the patch or update that the vendor develops toward mitigating the problem.
2. Generally, when the vendor releases the patch or update, ICS-CERT releases an advisory containing vulnerability characterization and exploitability as well as affected product information with specific mitigation strategies for users. However, because the vulnerability is not yet known publicly, ICS-CERT releases this advisory to the US-CERT secure portal library, which is available only to a limited vetted membership—primarily CIKR asset owners, federal, state, local, and tribal agencies. ICS-CERT provides updates to portal advisories as needed.
3. ICS-CERT generally coordinates the initial advisory release to the secure portal library to coincide with the vendor's patch or update release.
4. ICS-CERT negotiates a product update period following the initial portal release, to allow time for the vendor's users to obtain and install the patch or update. After the product update period has passed, ICS-CERT releases the advisory to the ICS-CERT web page for public disclosure.

A recent example of a unique vulnerability disclosure case is a situation involving multiple vulnerabilities in a major programmable logic controller (PLC) vendors' equipment.

(continued on page 3)

(from page 2)

This process began as a coordinated disclosure with researcher Dillon Beresford of NSS Labs, Siemens AG, and ICS-CERT. After coordinating mitigation development efforts for the reported vulnerabilities, Mr. Beresford indicated that he planned a high-level presentation, including a demonstration of the reported vulnerabilities, at a security conference. ICS-CERT sent a representative with vulnerability handling experience to attend Mr. Beresford's presentation and possibly answer questions about vulnerability disclosures and the disclosure process from the ICS-CERT perspective. Subsequently, Mr. Beresford determined that making his information public was not in the best interest of control system cybersecurity; he cancelled his talk until further discussions with the vendor regarding mitigations could take place. ICS-CERT supports Mr. Beresford's decision to pull his presentation and continues to work with him and Siemens to develop effective mitigations for the reported vulnerabilities and pass information regarding the progress of this issue to the ICS community. ICS-CERT considers the situation described above a validation of the coordinated disclosure process and continues to work with Mr. Beresford and other researchers on coordinated disclosures of other vulnerabilities affecting ICS in critical infrastructure.

ICS-CERT highly values your thoughts and concerns about this vulnerability disclosure process, and appreciates your feedback. Please send suggestions to improve the vulnerability disclosure process to ics-cert@dhs.gov.

RECENT VULNERABILITY DISCLOSURE TRENDS

Vulnerability Disclosures—Coordinated vs. Unanticipated

Table 1 identifies the number of vulnerability tickets and disclosure efforts in which ICS-CERT has participated from January 1, 2011, through May 31, 2011. Table 2 identifies the number of vulnerability tickets and disclosure efforts for May 2011.

Table 1. Vulnerability disclosures by category, January-May 2011.

VU Tickets January-May 2011	Unanticipated	Coordinated	Alerts	Advisories
55	11	44	16	44

Table 2. Vulnerability disclosures by category, May 2011.

VU Tickets May 2011	Unanticipated	Coordinated	Alerts	Advisories
11	2	9	3	10

The total number of vulnerability tickets does not equal the total number of alerts and advisories as some are not directly related to vulnerability tickets.

Unanticipated —The number of disclosures is fewer than the number of published alerts because several alerts were published for general situational awareness rather than a specific vulnerability disclosure (FAA GPS Testing, Solar Storm Impact, etc.).

Coordinated —The number of disclosures is fewer than the number of published advisories because 12 advisories were published as follow-up reports to ICS-CERT alerts, and several advisories were published for general situational awareness rather than a specific vulnerability disclosure.

COORDINATED VULNERABILITY DISCLOSURE

ICS-CERT actively works with a variety of researchers and ICS vendors to foster coordinated vulnerability disclosure. The coordinated disclosure process allows time for a vendor to release patches and users to apply patches prior to public disclosure of the vulnerability.

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@dhs.gov or toll free at 1-877-776-7585.

Noted Coordinated Disclosure Researchers

ICS-CERT appreciates working through the coordinated disclosure process with approximately 10 different researchers in a coordinated manner on various vulnerability issues at this time. Please continue to monitor ICS-CERT webpage for additional information.

UPCOMING EVENTS

JUNE

Oil & Gas Cyber Security Summit
June 27–28, 2011
Houston, Texas

Joint Critical Infrastructure Protection (JCIP) Symposium
June 28, 2011
Newark, New Jersey

JULY

2011 Chemical Sector Security Summit
July 6–7, 2011
Baltimore, Maryland

The Advanced Training: Control Systems Cyber Security Advanced Training and Workshop
(1 week)
July 18–22, 2011
Idaho Falls, Idaho
Description:
http://www.us-cert.gov/control_systems/pdf/ICS_AdvancedTrainingInvite_July18-22_2011.pdf.

Joint Critical Infrastructure Protection (JCIP) Symposium
July 20–21, 2011
Atlanta, Georigia

HydroVision International
July 19–22, 2011
Sacramento, California

AUGUST

7th Annual Government Forum of Incident Response and Security Teams (GFIRST) National Conference
August 07–12, 2011
Nashville, Tennessee
Description:
http://www.us-cert.gov/GFIRST/pre-conference.html

RECENT PRODUCT RELEASES

ALERTS

Alert "ICS-ALERT-11-131-01 - Advantech Studio ISSymbol ActiveX Control Buffer Overflow"
ICS-CERT is aware of a report of multiple buffer overflow vulnerabilities in Advantech ISSymbol ActiveX Control 61.6.0.0 and Advantech Studio 6.1 SP6 Build 61.6.01.05. Boundary errors that occur during various functions can cause heap-based or stack-based overflows, which in turn allow execution of arbitrary code. Secunia recommends that users set the kill-bit for the affected ActiveX control to mitigate this vulnerability.

Alert "ICS-ALERT-11-129-01 - Samsung Data Management Server Root Access"
ICS-CERT has been notified of a root access vulnerability in the Samsung DMS product.

ADVISORIES

Advisory "ICSA-11-147-01A - Ecava IntegraXor DLL Hijacking"
This update contains the revised location for the patch.

Advisory "ICSA-11-147-02 - Ecava IntegraXor XSS"
ICS-CERT has become aware of multiple Denial of Service (DOS) vulnerabilities in 7T IGSS SCADA HMI. 7T has developed a patch that resolves the reported vulnerabilities. ICS-CERT has validated this patch.

Advisory "ICSA-11-147-01 - Ecava IntegraXor DLL Hijacking"
ICS-CERT has become aware of several cross site scripting (XSS) vulnerabilities in the Ecava IntegraXor SCADA product. ICS-CERT has validated the patch.

Advisory "ICSA-11-132-01 - 7-Technologies IGSS DoS"
ICS-CERT has become aware of multiple Denial of Service (DOS) vulnerabilities in 7T IGSS SCADA HMI. 7T has developed a patch that resolves the reported vulnerabilities. ICS-CERT has validated the patch.

Advisory "ICSA-11-131-01 - ICONICS GENESIS32 and BizViz ActiveX Stack Overflow"
Security researchers Scott Bell and Blair Strang of Security-Assessment.com have released a report detailing a stack overflow vulnerability that affects ICONICS WebHMI, GENESIS32, GENESIS64 and BizViz products. The vulnerable ActiveX control, GenVersion.dll, can be exploited allowing remote code execution.

Advisory "ICSA-11-069-01A - (UPDATE) Samsung Data Management Server"
This Updated Advisory updates the independent researcher attribution.
(http://www.SecurityByDefault.com).

Advisory "ICSA-11-126-01 - 7-Technologies IGSS Multiple Vulnerabilities"
An independent researcher has identified eight vulnerabilities in 7-Technologies (7T) IGSS SCADA human-machine interface (HMI) application. Each of the identified vulnerabilities includes proof-ofconcept (PoC) exploit code.

Advisory "ICSA-11-069-01 - Samsung Data Management Server"
Jose Antonio Guasch, an independent security researcher with Sistemas Informaticos Abiertos (SIA), reported a SQL injection vulnerability in the Samsung Data Management Server (DMS). Samsung has released the validated patch.

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

Disclaimer: *ICS-CERT compiles this section from multiple resources including current events as disclosed on websites, blogs, mailing lists, and at conferences. ICS-CERT does not endorse the opinions or comments stated in these articles, nor has the US Department of Homeland Security (DHS) independently verified the technical information included. The links provided were confirmed at the time of data capture. ICS-CERT is not responsible for broken or nonfunctioning URLs.*

FERC Looks for New Authority in Cybersecurity Legislation

May 09, 2011

"As various Senate panels try to come to agreement over a comprehensive bill, the Federal Energy Regulatory Commission is saying it needs its enhanced ability to protect the networks controlling electrical grids from potential electromagnetic pulses from solar flares and other causes."

http://www.powergenworldwide.com/index/display/wire-news-display/1414135760.html.

DOCUMENT FAQ

What is the publication schedule for this digest?

The ICS-CERT publishes the "ICS-CERT Monthly Monitor" approximately 12 times per year. Each issue includes information collected in the previous month.

The public can view this document at the ICS-CERT web page http://www.ics-cert.org

The ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets.

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

ICS-CERT warns of critical industrial control bug

May 12, 2011

The [Industrial Control Systems] Cyber Emergency Response Team is warning oil refineries, power plants, and other industrial facilities of a bug in a popular piece of software that could allow attackers to take control of their computer systems.

http://www.theregister.co.uk/2011/05/12/critical_iconics_scada_bug/.

U.S. Outlines Cybersecurity Initiative

May 12, 2011

"Private companies that manage the nation's "critical infrastructure" would be required under a new cybersecurity initiative announced Thursday by the White House to submit detailed plans showing how they can defend themselves against cyber attack."

http://www.npr.org/2011/05/12/136250408/obama-lays-out-cybersecurity-plan.

White House cyber plan would expand role of DHS, private sector

May 13, 2011

The Obama administration is proposing comprehensive cybersecurity legislation that would clarify the government's role in protecting the nation's critical infrastructure and favor public/private cooperation over regulation.

http://gcn.com/articles/2011/05/12/white-house-cybersecurity-proposal.aspx.

Code Wars: America's Cyber Threat

May 18, 2011

"In the United States, we are Internet dependent. Our financial systems, power grids, telecommunications, water supplies, flight controls and military communications are all online – making them vulnerable to countless attacks by cyber criminals."

http://www.cnbc.com/id/42210831/.

Fieldbus Foundation Announces Latest Enhancements to FOUNDATION Fieldbus Specifications

May 19, 2011

"The Fieldbus Foundation announced enhancements to its open, non-proprietary FOUNDATION fieldbus physical layer technology. The latest updates to the H1 (31.25 kbit/s) physical layer specifications will improve the robustness of fieldbus control systems by optimizing device interoperability and integration."

http://www.arcweb.com/Regions/North_America/archive/2011/05/17/fieldbus-foundation-announces-latest-enhancements-to-foundation-fieldbus-specifications.aspx.

Common Vulnerability Reporting Framework

May 20, 2011

"A new vulnerability reporting framework was announced this week to standardize security vulnerability reporting. The Common Vulnerability Reporting Framework (CVRF) is an XML-based language that will enable different stakeholders across different organizations to share critical security-related information in a single format, speeding up information exchange and digestion."

http://isc.sans.edu/index.html.

Backdoor instructions for Allied Telesis switches leaked

May 30, 2011

"A simple categorizing mistake has resulted in the publishing of an internal Allied Telesis document that reveals how to set up backdoor accounts for the company's switches."

http://www.net-security.org/secworld.php?id=11089.

Cyber Combat: Act of War

May 31. 2011

"The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force."

http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html?mod=WSJ_hp_LEFTTopStories.