Industrial Control Systems

Weekly Situational Awareness Report

Week ending 13 January 2013

Register for a one-month trial subscription
Of this weekly NexDefense intelligence report

Please Contact Michael Radigan or visit www.nexdefense.com

Michael Radigan | NexDefense | 614-942-0919
michael.radigan@nexdefense.com

Powered By

This document provides cyber threat and vulnerability intelligence for industrial control system (ICS) stakeholders. Contents focus on potential attack group interest, capability, and opportunity, and may serve as indicators and warnings of ICS cyber incidents. Control systems security stakeholders may use this information to support operational risk management decisions.

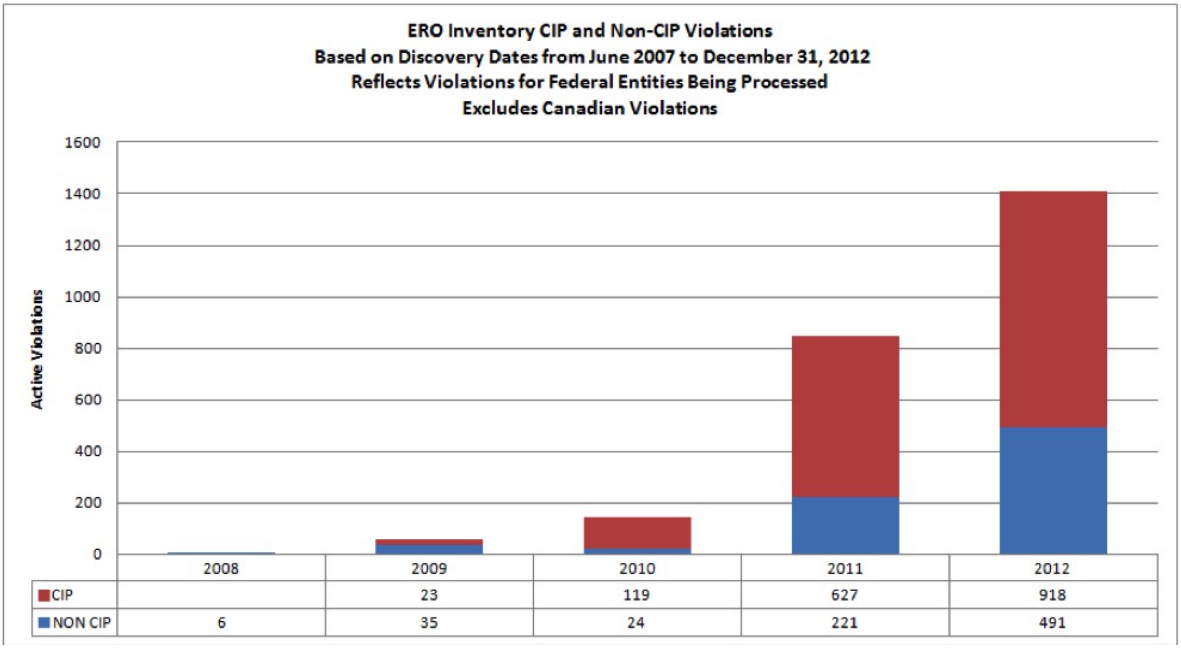
Table of Contents

ICS Indications and Warnings Update

This section summarizes the threat and vulnerability indications recognized during the period of this report. Critical Intelligence monitors open sources for information regarding potential adversary interest, capability and opportunity to perform a cyber attack on industrial control systems (ICS).

NERC CIP violations trend upwards in 2012, huge fines – Jan. 08

A presentation on violations of the North American Electric Reliability Corporation (NERC) revealed that violations of the Critical Infrastructure Protection (CIP) standards are an increasing load for regulators - up 46% from 2012, as seen in the graph below [1].



Also during the year NERC levied a pair of large fines for CIP violations, one against an entity belonging to the RFC region ($725,000) and one against and entity belonging to SERC region ($950,000) [2].

The experience of the NERC CIP regulatory regime provides insight into what future regimes, such as those proposed by U.S. legislators [3], might involve.

[1] http://www.nerc.com/files/BOTCC-%20Key%20Compliance%20Trends-%20January%202%202013%20-Mike%20Farzaneh%20reviewed.pdf
[2] http://www.nerc.com/filez/enforcement/index.html
[3] http://thomas.loc.gov/cgi-bin/query/z?c112:S.2105:

ICS Technical and Market Developments

This section identifies technical developments in industrial control systems or other fields that may have important cyber security consequences for ICS.

Title	**IPKeys Technologies Teams with Connexx Energy on OpenADR 2.0 Driver Software for Niagara AX**
Date	January 8, 2013
Sector:	Building Automation
Analysis	This press release describes efforts that will further commercialize the OpenADR communications protocol: *IPKeys Technologies, an expert in Smart Grid communications technology and Connexx Energy, Inc., a subsidiary of Lynxspring, Inc. and leading developer of open technologies for building automation and energy management solutions today announced that they will partner to deliver an OpenADR 2.0 a-certified Virtual End Node (VEN) driver for the Niagara AX® platform. Through this solution, IPKeys Technologies and Connexx Energy will provide an OpenADR 2.0a-certified driver for Niagara AX®, permitting rapid deployment of standards-based AutoDR solutions to the Niagara community and enabling the collaborative facility-grid relationship necessary to make Smart Grid a reality. [1]* Several important utilities have already announced plans to adopt OpenADR as a standard [2], which provides electricity and service providers the ability to send load shedding commands. The Niagara framework is already deployed in over 300,000 systems worldwide – usually for building automation [3]. Numerous vulnerabilities have been found Niagara software to date [4-5]. Niagara products are often connected directly to the Internet [6]. The creation of OpenADR drivers for the Niagara framework may pave the way for Niagara to be used with devices that are often turned off in demand response situations -- such as in-home air conditioner units. If trends of attaching these Niagara Framework devices to the Internet continues, these air conditioners may also be connected.
References	[1] http://www.tridium.com/cs/tridium_news/press_release_detail?pressrelease.id=522 [2] http://finance.yahoo.com/news/leading-utilities-embrace-openadr-2-160950750.html [3] http://www.tridium.com/cs/tridium_news/press_release_detail?pressrelease.id=465 [4] https://www.tridium.com/galleries/briefings/NiagaraAX_Framework_Software_Security_A

	lert.pdf [5] http://xs-sniper.com/blog/2012/11/26/tridium-niagara-directory-traversal/ [6] http://www.shodanhq.com/?q=niagara

Title	**Vulnerability of oil and gas infrastructure drives security investments**
Date	January 15, 2013
Sector:	Gas and Oil
Analysis	*New analysis from Frost & Sullivan finds that the market earned revenues of $18.31 billion in 2011 and estimates this to reach $31.27 billion in 2021. [1]* Such investment likely has to do with the success of targeted attacks against oil firms, as noted in the popular press over the past years: Conoco Phillips, Marathon Oil, Exxon Mobil, others [2-3]. The American Gas Association recently issued a statement concerning their commitment to cyber security as a result of recent attacks [4]. Similar predictions for increased security spending in the electricity sector have been recently advanced [5].
References	[1] http://www.net-security.org/secworld.php?id=14238&utm_medium=twitter&utm_source=dlvr.it [2] http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved [3] http://online.wsj.com/article/SB123914805204099085.html [4] http://www.platts.com/RSSFeedDetailedNews/RSSFeed/NaturalGas/8961076 [5] http://www.pikeresearch.com/research/smart-grid-cyber-security

ICS Software and Firmware Updates

This section includes information on recent ICS software and firmware updates from leading vendors. Updates may address security issues even when these are not described in release notes. Visiting the update Web site may require an account with the vendor.

Vendor	*Product*	*Date*
GarrettCom	Consolidated MIB MNS-6K MIB (for release v4.4.3)	1/13/13
GarrettCom	Magnum MNS-DX Management Software (DX40/940/1000) v3.1.7	1/10/13
GI intelligent Platforms	Historian 5.0 SIM1	1/11/13
GI intelligent Platforms	Historian 4.5 SIM-14	1/10/13
Honeywell	** Microsoft Security Hot-fixes Honeywell Qualification Matrix	1/11/13
National Instruments	NI-SWITCH .NET Class Libraries 1.0	1/11/13
National Instruments	NI-DCPower .NET Class Libraries 1.0	1/18/13
National Instruments	NI-USRP 1.2 - Windows 7 32-bit/Vista 32-bit/XP (SP2) 32-bit/Vista 64-bit/7 64-bit	1/09/13
National Instruments	NI PXIe-6544/6545/6547/6548 Firmware 12111620	1/13/13
National Instruments	NI PXIe-6555/6556 Firmware 12111620	1/10/13
OSIsoft	PI OLEDB Enterprise 2012	1/14/13
OSIsoft	PI Tag Export Utility for AX-S4 61850 1.0.0.6	1/10/13
OSIsoft	PI Interface for DNP 3.0 v3.1.1.45	1/10/13
OSIsoft	PI ProcessBook 2012 SP1	1/10/13
OSIsoft	MS Security Patch Compatibility	1/10/13

Rockwell Automation	FactoryTalk Historian SE v3.01	1/11/13
Siemens	Basis Firmware Update for CP 441	1/07/13
Siemens	** Security Update for SIMATIC RF-MANAGER Professional and RF-MANAGER Basic	1/10/13
Siemens	COMOS-Information V9.2: Update/Service Pack	1/11/13j
Schneider Electric	** ClearSCADA Patch Testing-Jan2013.pdf	1/11/13
CygNet	** Microsoft patch testing for CygNet SCADA ABFTWUHist_20130108	1/15/13
Schneider Electric	IMS0LW10-1V Frmware 1.8.2.18.8271	01/09/13
Schneider Electric	Sarix Reset Device Script for 1.8.2.18 firmware	01/10/13
Schneider Electric	VAMPSET Setting Software Installation v2.2.112	01/11/13
Schneider Electric	Connexium Ethernet Configuration Software version 2.2.05	01/11/13
Schneider Electric	Unity Pro_V7.0_HF20050784	01/14/13
Schneider Electric	Unity Pro_V7.0 TimeStamping HotFix (Unity Pro_V7.0_HF1) and firmware update	01/14/13

** Known to be security related

Developments in ICS Defense

This section describes developments in ICS Defense identified during the reporting period. Stakeholders may use this section to identify security tools, functionality, or groups that may aid in enhancing ICS security.

SCADA Stangelove releases hardening guide for Siemens WinCC – Dec. 27

SCADA Strangelove, a group of Russian researchers who have recently focused attention on Siemens Wincc automation system [1-3], released a 12-page "Siemens WinCC 7.x Security Hardening Guide" [4-5].

The Guide is not dissimilar to hardening guidance for other systems or servers [6-8].

The Guide includes the following sections:

- Operating System Configuration
- System Network Parameters Configuration
- DBMS Configuration
- Additional Security Tools
- Simatic WinCC System Parameters
- Simatic WinCC Logon Configurations
- Simatic WinCC Access Configurations
- Simatic WinCC Events Logging
- Simatic WinCC Project Control
- Simatic WinCC Webnavigator Screen Publishing

Importantly and interestingly, the authors point out that some things that might be considered less-secure to an IT security professional are necessary for proper WinCC operation. For example, the authors instruct users to "enable unsigned drivers installation"[5].

One weakness of the guide is that it tells the reader to follow Siemens specifications for some items, but does not provide links or instructions for accessing those resources.

Many of these options and features are explained in Siemens WinCC documentation [9-13], however, Positive Technologies has taken the step that Siemens never has in concisely compiling important items into a single document under the title "Security hardening." Other ICS vendors would do well to follow this track of thinking.

[1] http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-223158.pdf
[2] http://scadastrangelove.blogspot.com/2012/11/wincc-harvester.html
[3] http://events.ccc.de/congress/2012/Fahrplan/events/5059.en.html
[4] http://scadastrangelove.blogspot.com/2012/12/siemens-simatic-wincc-7x-security.html
[5] http://www.slideshare.net/qqlan/positive-technologies-wincc-security-hardening-guide
[6] http://technet.microsoft.com/en-us/library/dd277307.aspx
[7] https://www.suse.com/documentation/sles11/pdfdoc/book_hardening/book_hardening.pdf
[8] http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml
[9] http://support.automation.siemens.com/WW/llisapi.dll/csfetch/26462131/wp_sec_b.pdf
[10] http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&=en&objid=43876783&caller=view
[11] http://support.automation.siemens.com/WW/llisapi.dll/csfetch/26366540/ps7vir_e.pdf?func=cslib.csFetch&nodeid=26609551
[12] http://support.automation.siemens.com/US/llisapi.dll/44454273?func=ll&objId=44454273&objAction=csView&nodeid0=10806836&lang=en&siteid=cseus&aktprim=0&extranet=standard&viewreg=US&load=treecontent
[13] http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=28580051&caller=view

Singapore amends cyber law to protect critical infrastructures – Jan. 14

The city-state of Singapore passed legislation to empower state oversight of critical information infrastructures [1].

An official summary of the act includes the following:

> *Sub-section (1) of the new Section 15A empowers the Minister to issue a certificate to authorise or direct a person or an entity to take measures or comply with requirements necessary to prevent, detect or counter a threat to the national security, essential services, defence or foreign relations of Singapore.*
>
> *For example, a CII operator may be required to provide information relating to the design, configuration, operation and security of computers, computer programmes or computer services. This will help identify and address cyber threats and system vulnerabilities. A CII operator may also be required to report cybersecurity breaches to the Minister or an authorised public officer. This will provide situational awareness of cyber threats at the national level and help assessments on the need for further security measures. Before a certificate is issued by the Minister, CII stakeholders will be consulted on the implications, where practicable. The measures required under the certificate will be limited to what is necessary to safeguard national security, defence, foreign relations, or essential services.*
>
> *I want to emphasise that it is also in the interests of a CII stakeholder to proactively invest in preventive cybersecurity measures. This is because a successful cyber attack could lead to significant financial loss and reputational damage for the CII stakeholder. Hence, as domain owners responsible for the security of their assets, CII stakeholders will generally be expected to bear the cost of these measures.*
>
> *Given the severity of the threat that cyber attacks can pose to the nation, the new sub-section (4) makes it an offence if a person fails to take any measure, or comply with the directions of the Minister, under Section 15A of the Act. Similarly, non-compliance with the directions of a person who is acting pursuant to the certificate issued by Minister under Section 15A will also be an offence. It will also be an offence to obstruct a person from complying with the Minister's directions to him. These offences will be punishable with a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both.*
>
> *New sub-sections (6) and (7) confer various immunities for acts done in good faith pursuant to the Minister's certificate under Section 15A of the Act, including any direction given pursuant*

> *to such a certificate. This is necessary to ensure that those who are acting pursuant to the certificate or direction can perform their functions without being constrained for fear of civil or criminal liabilities.*
>
> *For example, if a malware is detected to be targeting a particular make and model of equipment used by our CII operators, the Minister may issue a certificate to the CII operators to direct that certain cybersecurity measures be taken. In the course of implementing these measures in good faith, if there is service degradation or disruption that results in the failure of the CII operators to meet their contractual Service Level Agreements with their customers, the CII operators can claim immunity in any legal proceedings against them by their customers. [2]*

It should be noted that Singapore generally emphasizes government and public good over individual rights. This bill is consistent with that approach [3].

Bills advanced in the United States for comprehensive cyber security and emergency powers have included some similar clauses empowering significant government oversight and granting authority give orders with penalties for non-compliance.

For example

- HR 2195, introduced in 2009, would have given the Federal Energy Regulatory Commission authority to issue rules and orders to any entity that controls, owns, or operates critical electric infrastructure to protect against vulnerabilities or threats, without prior notice in an emergency [4].
- S. 2105, introduced in 2012, would have required covered critical infrastructure operators to "report significant incidents" and given industry-specific regulators authority to institute "civil penalties" (fines) when violations occur and where the asset owner fails to remediate the violation in an "appropriate timeframe" [5].

Emergency powers clauses for responding to cyber attack are a tricky issue. How will a government entity who is far removed from day to day operations of critical infrastructures know what actions best meet engineering and business needs? How can emergency personnel with authority to make cyber orders completely understand the impact of an order? A third party will never be able to adequately manage risk; this requires competencies that are not aligned with government capability. The best defense is to ensure that asset owners have the ability to recognize and appropriately respond to cyber threats and incidents for themselves [1].

On the other hand, the fact that under the new Singapore law the government reserves the right to issue cyber "orders" may be a fair incentive by itself; asset owners may not want to face the consequences of having someone relatively clueless telling them what to do.

Singapore's officials who now wield the semi-coercive cyber power have promised to use it "judiciously" [6].

[1] http://www.todayonline.com/Singapore/EDC130114-0000115/Parliament-passes-amendments-to-Computer-Misuse-Act
[2] http://www.mha.gov.sg/news_details.aspx?nid=Mjc1NQ%3d%3d-OPxAwlOrs50%3d
[3] http://en.wikipedia.org/wiki/Singapore
[4] http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.2195:
[5] http://thomas.loc.gov/cgi-bin/query/z?c112:S.2105:
[6] http://www.mha.gov.sg/news_details.aspx?nid=Mjc1Nw%3d%3d-9trTx9rvq8c%3d

ICS-Specific Vulnerabilities

This section reports and provides analysis of control system specific vulnerabilities identified during the coverage period.

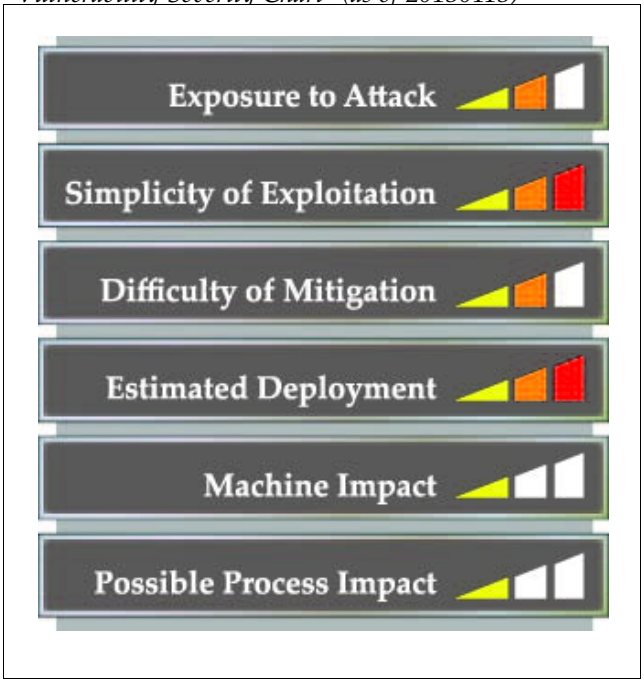
Rockwell Automation – EtherNet/IP information disclosure update

Versions affected:	1756-ENBT, 1756-EWEB, 1768-ENBT, 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter [1]
Approximate date public:	01/19/12 [2 (starting at minute 53:49)]
Sector primarily affected:	Multiple

Description:

An Information Disclosure of product-specific information unintended for normal use results when the affected product receives a malformed CIP packet. [1]

Vulnerability Severity Chart (as of 20130113)*



* See explanation at end of section

Exposure to attack: *Medium*

Under recommended practice configuration, an attacker must have access to the same network segment as the machine running the vulnerable software in order to exploit this vulnerability.

Simplicity of Exploitation: *High*

Technical details and proof of concept code are publicly available [3]. Digital Bond, which announced the vulnerabilities, has indicated that a Metasploit module to exploit this issue may be forthcoming [2].

Difficulty of mitigation: *Medium*

The vendor has released a patch to address this vulnerability for all affected products apart from 1788-ENBT and 1794-AENTR [1]. The updates can be download from Rockwell's website [5]. Rockwell has also made the following recommendations:

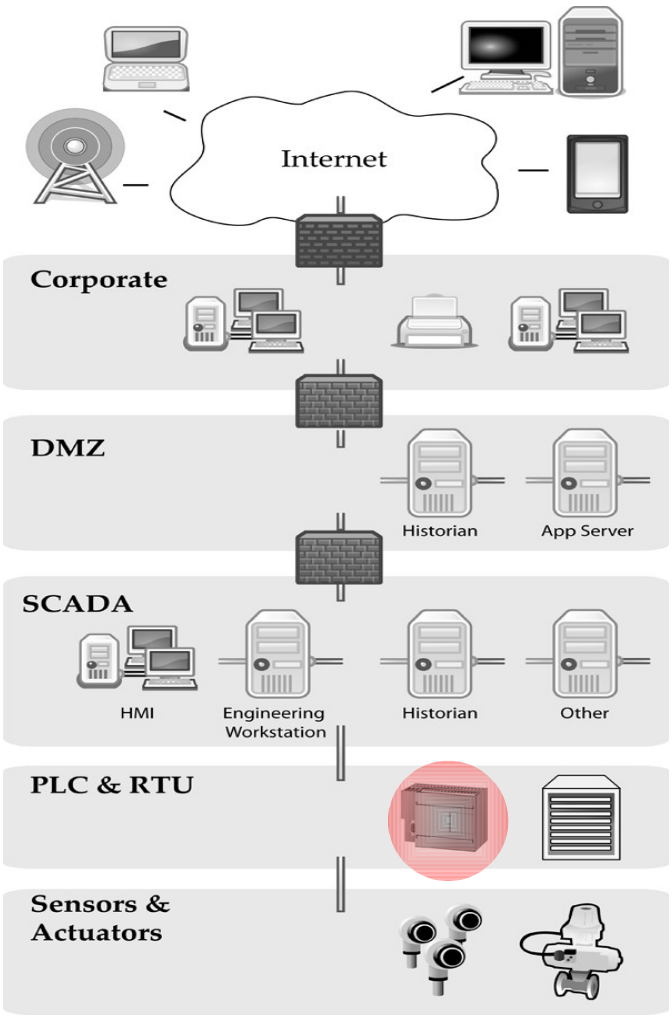
> *1. Block all traffic to the EtherNet/IP or other CIP protocol based devices from outside the Manufacturing Zone by restricting or blocking access to TCP and UDP Port# 2222 and Port# 44818 using appropriate security technology (e.g. a firewall, UTM devices, or other security appliance).*
>
> *2. Employ a Unified Threat Management (UTM) appliance that specifically supports CIP message filtering designed to block the specific vulnerabilities:*
>
> *CIP Ethernet configuration service*
>
> *Messages sent to CIP Class code: 0xc0 with Service code: 0x97 service*
>
> *CIP reset service*
>
> *CIP Ethernet configuration service*
>
> *NOTE: Rockwell Automation continues to investigate and evaluate other product-level strategies to address this vulnerability.*

Estimated deployment: *High*

Rockwell Automation is a U.S. based automation vendor. The firm's PLCs hold market leading

position in the North America. Rockwell products are used across a variety of infrastructure domains, though they are used more frequently for discrete industries than for process industries. As such they are more likely to be used in supporting functions in the electric, water, and petroleum sectors (such as fan operations, cooling towers, or lighting) than for controlling primary processes. ControlLogix is a product of Rockwell's Allen-Bradley line [4].

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



Machine impact: *Low*

Successful exploitation results in information disclosure [1,3]. The information gathered may be useful in developing an exploit that allows for execution of arbitrary code [2 at minute 1:01:30].

Possible process impact: *Low*

The information disclosure does not immediately affect the controlled process.

Additional analysis:

Port number (s) of affected service: 2222, 44818

A review of activity on these ports at the SANS Internet Storm Center show no recent spikes.

This vulnerability was discovered or disclosed by: Rubén Santamarta [3]

National Vulnerability Database: NA

ICS-CERT: www.us-cert.gov/control_systems/pdf/ICS-Alert-12-020-02.pdf
www.us-cert.gov/control_systems/pdf/ICS-Alert-12-020-02A.pdf
www.us-cert.gov/control_systems/pdf/ICSA-13-011-03.pdf

This exploit was disclosed by Digital Bond as part of the the Project Basecamp results presented at SCADA Security Scientific Symposium (S4) [2]. Ruben Santamarta calls this "Attack #4" [3]; Rockwell calls it "Vulnerability 2" [1].
This vulnerability was reported previously in the 20120129 Weekly Report.

Sources

[1] http://rockwellautomation.custhelp.com/app/answers/detail/a_id/470154
[2] http://vimeopro.com/user10193115/s4-2012/video/35783988
[3] http://reversemode.com/downloads/logix_report_basecamp.pdf
[4] http://ab.rockwellautomation.com/Programmable-Controllers/ControlLogix
[5] http://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx

Rockwell Automation – EtherNet/IP ci_ParseSegment function denial of service update

Versions affected: 1756-ENBT, 1756-EWEB, 1768-ENBT, 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter [1]

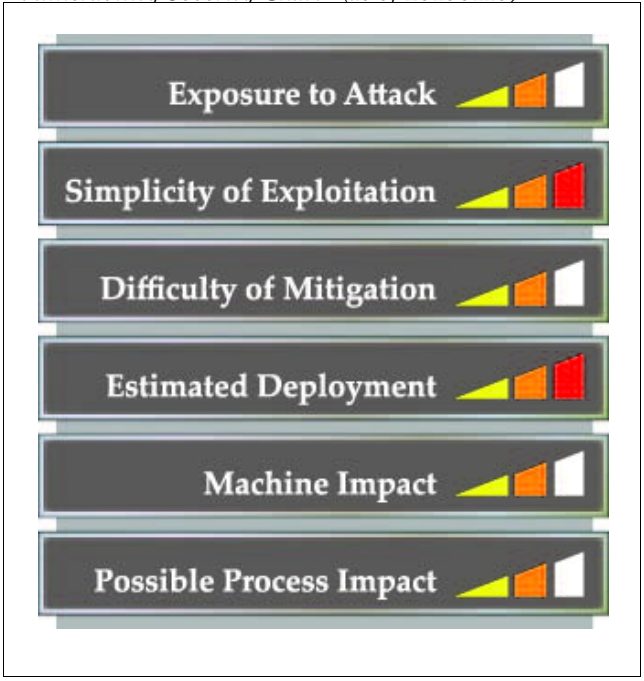
Approximate date public: 01/19/12 [2 (starting at minute 53:49)]

Sector primarily affected: Multiple

Description:

A Denial of Service (DOS) condition and a product recoverable fault results when affected product receives a malformed CIP packet. Receipt of such a message from an unauthorized source has will cause a disruption of communication to other products in controller platform or system. Recovery from a successful exploitation of this vulnerability requires the product to be reset via power cycle to the chassis or removal-reinsertion of module [1].

Vulnerability Severity Chart (as of 20130113)*



* See explanation at end of section

Exposure to attack: *Medium*

Under recommended practice configuration, an attacker must have access to the same network segment as the machine running the vulnerable software in order to exploit this vulnerability.

Simplicity of Exploitation: *High*

Technical details and proof of concept code are publicly available [3]. Digital Bond, which announced the vulnerabilities, has indicated that a Metasploit module to exploit this issue may be forthcoming [2].

Difficulty of mitigation: *Medium*

The vendor has released a patch to address this vulnerability for all affected products apart from 1788-ENBT and 1794-AENTR [1]. The updates can be download from Rockwell's website [5]. Rockwell has also made the following recommendations:

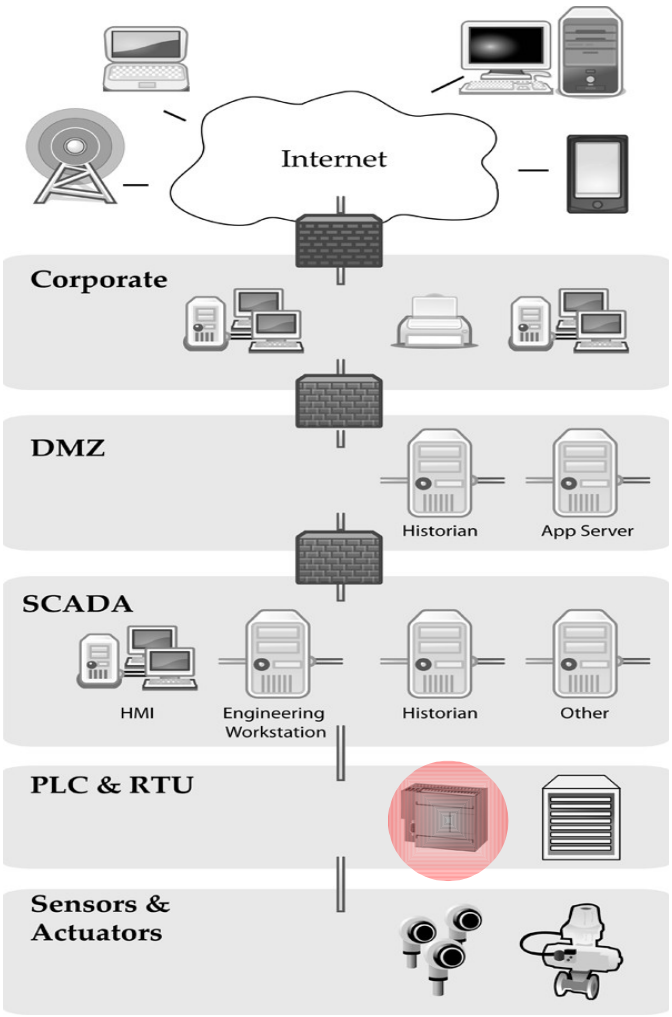
> *1. Block all traffic to the EtherNet/IP or other CIP protocol based devices from outside the Manufacturing Zone by restricting or blocking access to TCP and UDP Port# 2222 and Port# 44818 using appropriate security technology (e.g. a firewall, UTM devices, or other security appliance).*
>
> *2. Employ a Unified Threat Management (UTM) appliance that specifically supports CIP message filtering designed to block the specific vulnerabilities:*
>
> *CIP Ethernet configuration service*
>
> *Messages sent to CIP Class code: 0xc0 with Service code: 0x97 service*
>
> *CIP reset service*
>
> *CIP Ethernet configuration service*
>
> *NOTE: Rockwell Automation continues to investigate and evaluate other product-level strategies to address this vulnerability.*

Estimated deployment: *High*

Rockwell Automation is a U.S. based automation vendor. The firm's PLCs hold market leading

position in the North America. Rockwell products are used across a variety of infrastructure domains, though they are used more frequently for discrete industries than for process industries. As such they are more likely to be used in supporting functions in the electric, water, and petroleum sectors (such as fan operations, cooling towers, or lighting) than for controlling primary processes. ControlLogix is a product of Rockwell's Allen-Bradley line [4].

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



Machine impact: *Medium*

Successful exploitation results in denial of service.

Possible process impact: *Medium*

In case of successful exploitation, the PLC ceases to function. Impacts will vary by process.

Additional analysis:

Port number (s) of affected service: 2222, 44818

A review of activity on these ports at the SANS Internet Storm Center show no recent spikes.

This vulnerability was discovered or disclosed by: Rubén Santamarta [3]

National Vulnerability Database: NA

ICS-CERT: www.us-cert.gov/control_systems/pdf/ICS-Alert-12-020-02.pdf
www.us-cert.gov/control_systems/pdf/ICS-Alert-12-020-02A.pdf
www.us-cert.gov/control_systems/pdf/ICSA-13-011-03.pdf

This exploit was disclosed by Digital Bond as part of the the Project Basecamp results presented at SCADA Security Scientific Symposium (S4) 2012 [2]. Ruben Santamarta calls this "Attack #6" [3]; Rockwell calls it "Vulnerability #4" [1].

This vulnerability was reported previously in the 20120129 Weekly Report.

Sources

[1] http://rockwellautomation.custhelp.com/app/answers/detail/a_id/470154
[2] http://vimeopro.com/user10193115/s4-2012/video/35783988
[3] http://reversemode.com/downloads/logix_report_basecamp.pdf
[4] http://ab.rockwellautomation.com/Programmable-Controllers/ControlLogix
[5] http://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx

Rockwell Automation – Automation MicroLogix Web server weak authentication update

Versions affected: MicroLogix 1100, MicroLogix 1400 [1].

Approximate date public: 01/19/12 [2 (starting at minute 1:04:13:)

Sector primarily affected: Multiple

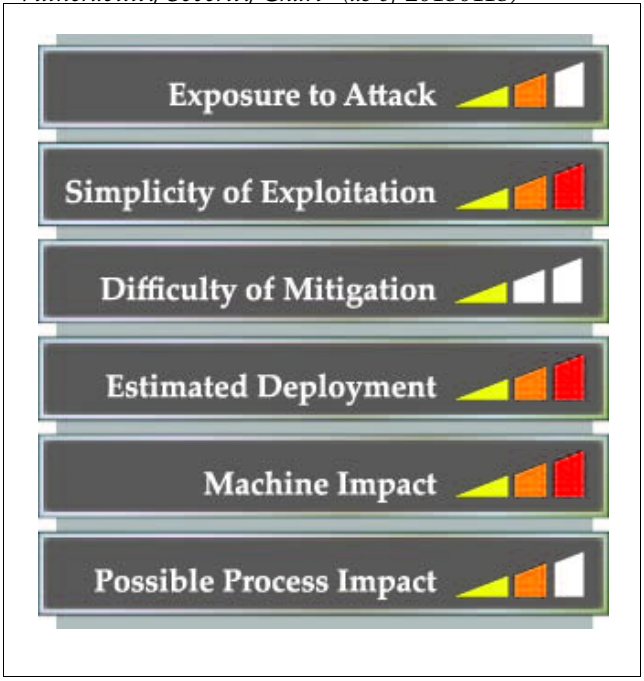
Description:

The webserver password authentication mechanism employed by the affected products is vulnerable to a Man-in-the-Middle (MitM) and Replay attack. Successful exploitation of this vulnerability will allow unauthorized access of the product's webserver to view and alter product configuration and diagnostics information [1].

Jacob Kitchel, who disclosed this vulnerability stated:

"The nonce is hard-coded and static across reboots, which basically allows you to capture the request once and replay it an infinite number of times as long as the password is the same. And it allows you to manually generate the responses and develop a brut force tool to figure out the password for the Web interface [2].

Vulnerability Severity Chart (as of 20130113)*



* See explanation at end of section

Exposure to attack: *Medium*

Under recommended practice configuration, an attacker must have access to the same network segment as the machine running the vulnerable software in order to exploit this vulnerability.

Simplicity of Exploitation: *High*

Technical details and proof of concept code are publicly available [3]. Digital Bond, which announced the vulnerabilities, has indicated that a Metasploit module to exploit this issue may be forthcoming [2].

Difficulty of mitigation: *Low*

The vendor has issued a patch to address this issue [1]. The latest MicroLogix firmware can downloaded from Rockwell's website [4]. It does, however, make the following recommendations and notes:
1. Where possible for affected products, disable the web server in the Ethernet Channel 1 configuration in RSLogix 500 software. This is done by unchecking the HTTP Server Enable checkbox (checked by default) and power cycling the controller.

2. Change all default Administrator and Guest passwords.

3. If webserver functionality is desired in the MicroLogix 1100 or 1400 controllers, we recommend the product's firmware be upgraded to the most current version that includes enhanced protections including:

a. When a controller receives two consecutive invalid authentication requests from any HTTP client, the controller resets the Authentication Counter after 60 minutes.

b. When a controller receives 10 invalid authentication requests from any HTTP client, it will not accept any valid or invalid Authentication packets until a 24-hour HTTP Server Lock Timer timeout.

WARNING/REMINDER: Upgrading the controller firmware clears the web server configuration. It is necessary to manually

record the web server settings prior to a firmware upgrade so the configuration can be manually re-entered into the web server settings after the firmware upgrade is complete.

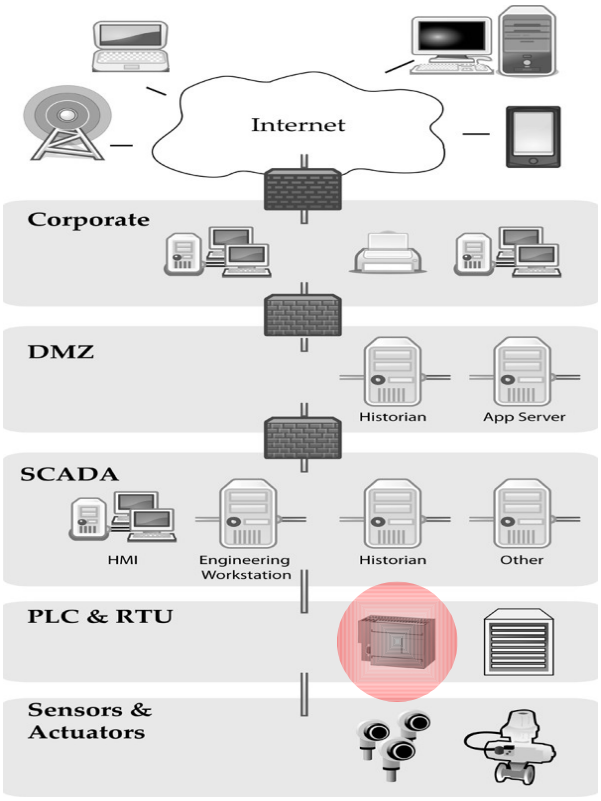
NOTE: The latest MicroLogix 1100 and 1400 firmware versions are posted at: http://www.ab.com/linked/programmablecontrol/plc/micrologix/downloads.html

4. If webserver functionality is desired in the MicroLogix 1100 or 1400 controllers, we recommend you configure User Accounts to only provide READ access to the product (e.g. do not configure READ/WRITE for Users). In addition, where possible exclusively access the product via User Accounts to minimize potential for a Replay attack to the Administrator's account. User-administration is done through the product's webserver.

Estimated deployment: *High*

Rockwell Automation is a U.S. based automation vendor. The firm's PLCs hold market leading position in the North America. Rockwell products are used across a variety of infrastructure domains, though they are used more frequently for discrete industries than for process industries. As such they are more likely to be used in supporting functions in the electric, water, and petroleum sectors (such as fan operations, cooling towers, or lighting) than for controlling primary processes.

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



Machine impact: *High*

Successful exploitation results in denial of service.

> *Recovery from successful exploitation of this vulnerability may require the product to be reset to its factory-default settings [1].*

Possible process impact: *Medium*

In case of successful exploitation, the PLC ceases to function. Impacts will vary by process.

Additional analysis:

Port number (s) of affected service: 2222, 44818

A review of activity on these ports at the SANS Internet Storm Center show no recent spikes.

This vulnerability was discovered or disclosed by: Jacob Kitchel [2]

National Vulnerability Database: NA

ICS-CERT: www.us-cert.gov/control_systems/pdf/ICS-Alert-12-020-02.pdf
www.us-cert.gov/control_systems/pdf/ICS-Alert-12-020-02A.pdf
www.us-cert.gov/control_systems/pdf/ICSA-13-011-03.pdf

This vulnerability was disclosed as part of the the Project Basecamp results presented at SCADA Security Scientific Symposium (S4) 2012 [2]. Micrologix is noted to have had authentication issues in the past [3].

Sources

[1] http://rockwellautomation.custhelp.com/app/answers/detail/a_id/470156
[2] http://vimeopro.com/user10193115/s4-2012/video/35783988
[3] http://rockwellautomation.custhelp.com/app/answers/detail/a_id/65980
[4] http://www.ab.com/linked/programmablecontrol/PLC/MicroLogix/downloads.html

Schneider Electric – IGSS buffer overflow

Versions affected: At least versions 8, 9, and 10 [1]. Prior versions may also be affected.

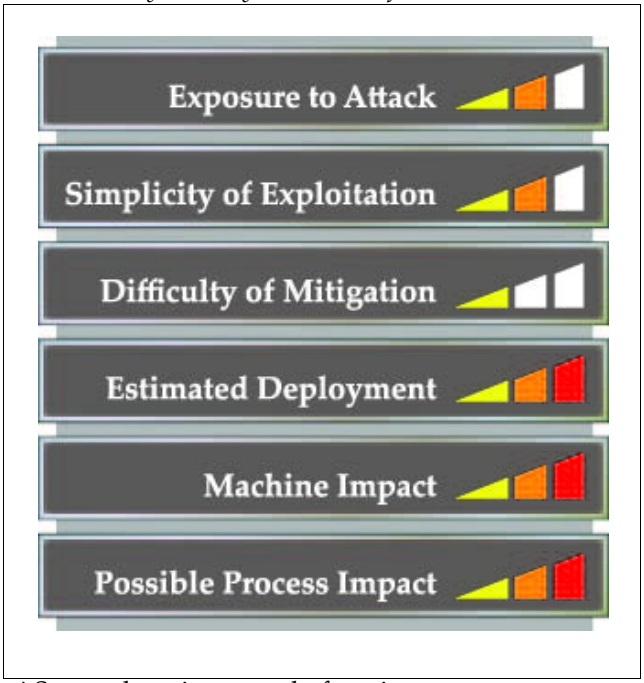
Approximate date public: 1/11/13

Sector primarily affected: Multiple

Description:

A buffer overflow vulnerability has been discovered in Schneider Electric's (formerly 7-Technologies) IGSS application that occurs "when parsing an incoming request through a TCP port into the IGSS element containing the vulnerability". Exploitation of the vulnerability allows for "denial of service and/or arbitrary code execution under the context of the user running the service (Administrator on a default installation)" [1-2].

Vulnerability Severity Chart (as of 20130113)*



* See explanation at end of section

Exposure to attack: *Medium*

Under recommended practice configuration, an attacker must have access to the same network segment as the machine running the vulnerable software in order to exploit this vulnerability.

Simplicity of Exploitation: *Medium*

The vulnerable component (dc.exe) and port (12397) are known [6].

Difficulty of mitigation: *Low*

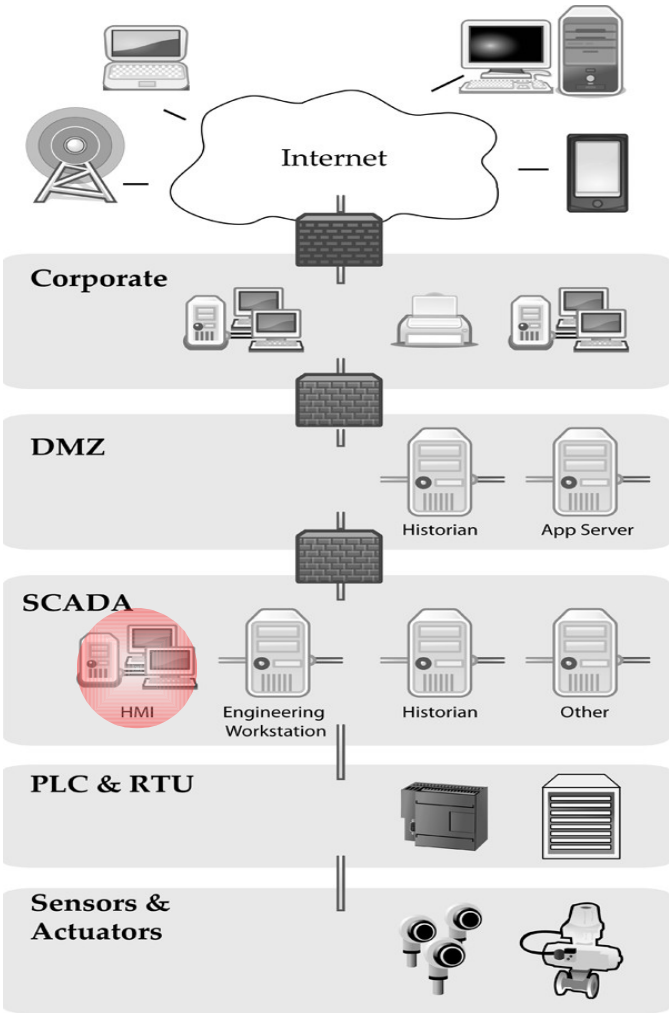
The vendor has released a patch to address this vulnerability for versions 8, 9, and 10. It is currently unclear if earlier versions exhibit this vulnerability. The patch can be obtained through IGSS's Update functionality [1], or downloaded from Schneider Electric's website (only for

Versions 9 and 10) [5].

Estimated deployment: *High*

IGSS was originally a product from the Danish SCADA/HMI vendor, 7-Technologies. The company specialized in products that served district heating, water, and manufacturing environments. In August 2011, 7-Technologies was acquired by the French electric engineering company, Schneider Electric [3]. IGSS is used in a variety of industries, from building automation, to electric power, to oil and gas. The company claims 28,000 installations in 47 countries. Installations appear concentrated in Denmark, Netherlands, and Sweden [4].

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



Machine impact: *High*

Successful exploitation could allow for denial of service and possible "arbitrary code execution under the context of the user running the service", which is Administrator by default.

Possible process impact: *High*

As successful exploitation could allow for arbitrary code execution on an HMI machine, an attacker could leverage this vulnerability to interact with the controlled process at will at the permission level of the current user or process, which is Administrator by default.

Additional analysis:

Port number (s) of affected service: 12397

This vulnerability was discovered or disclosed by: Aaron Portnoy of Exodus Intelligence [2, 6]

National Vulnerability Database:

ICS-CERT:

Sources

[1] http://igss.schneider-electric.com/products/igss/company/igss-news/13-01-11/Security_Update_for_IGSS.aspx
[2] http://www2.schneider-electric.com/corporate/en/support/cybersecurity/viewer-news.page?c_filepath=/templatedata/Content/News/data/en/local/cybersecurity/general_information/2013/01/20130110_advisory_of_vulnerability_affecting_igss_scada_software.xml
[3] http://en.wikipedia.org/wiki/Schneider_Electric
[4] http://www.igss.com/references/reference-list.aspx
[5] http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cyber-security-vulnerabilities-sorted.page
[6] http://secunia.com/advisories/51819/

Schneider Electric – Schneider Electric Software Update Utility (SESU) authenticated communications risk

Versions affected:

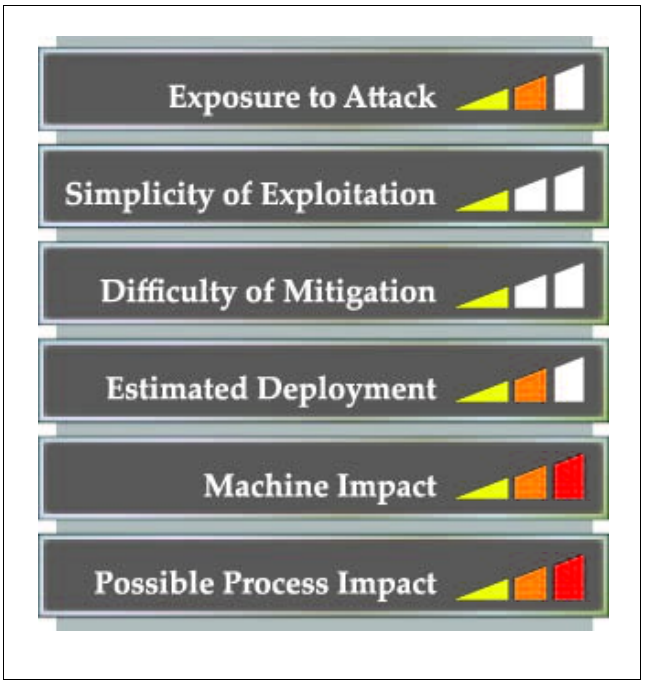
- IDS version 1.0 and 2.0
- PowerSuite version 2.5
- Smart Widget Acti 9, H8035, H8036, PM210, PM710, and PM750 version 1.0.0.0
- SoMachine version 1.2.1
- Spacial.pro versions 1.0.0.x
- SESU versions 1.0.x and 1.1.x
- Unity Pro version 5.0, 6.0, 6.1, and 4.1
- Vijeo Designer versions 6.0.x, 6.1.0.x, 5.0.0.x, and 5.1.0.x
- Vijeo Designer Opti versions 6.0.x, 5.1.0.x, and 5.0.0.x
- Web Gate Client Files version 5.1.x

Approximate date public: 12/20/12

Sector primarily affected: Multiple

Description:

Schneider Electric's Schneider Electric Software Update utility (SESU) utilizes a "a non signed communication between the SESU client on the customer PC and the Software Update server. Under certain circumstances and conditions this communication has the potential to execute arbitrary code on a vulnerable system which could result in unexpected consequences" [1].



Vulnerability Severity Chart (as of 20130113)*

Exposure to attack: *Medium*

Under recommended practice configuration, the vulnerable system should not be accessible via less-trusted networks.

Simplicity of Exploitation: *Low*

Additional details concerning the vulnerability are limited.

Difficulty of mitigation: *Low*

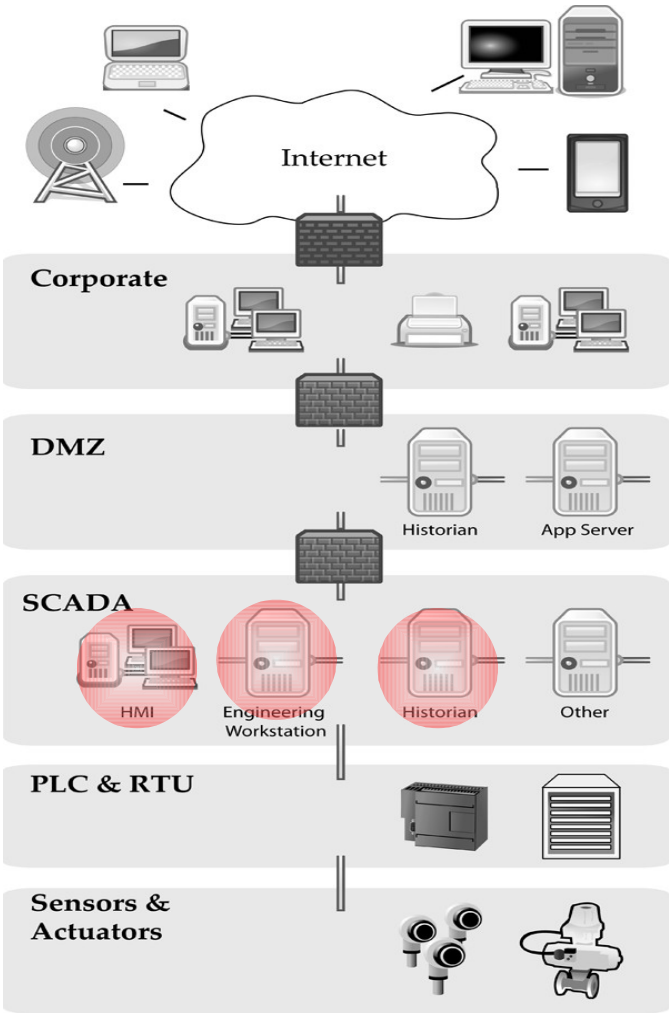
The vendor has developed a patch to address this vulnerability, by ensuring the SESU Client only utilizes HTTPS , ensuring signed communication [1]. Schneider Electric announced that the upgraded version would be available to customers in January 2013.

* See explanation at end of section

Estimated deployment: *Medium*

Schneider Electric is a world leading automation vendor headquartered in France. SESU is a "centralized update mechanism for updating Schneider software on a Windows PC. The software on the customer PC uses the update service as the mechanism of communication with the update server in order to receive periodic software updates" [1].

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



Machine impact: *High*

Successful exploitation allows for arbitrary code execution.

Possible process impact: *High*

A successful exploitation allows for arbitrary code execution on such a variety of devices, impact will vary by process.

Additional analysis:

Port number (s) of affected service: 80/TCP

This vulnerability was discovered or disclosed by: Arthur Gervais

National Vulnerability Database:

ICS-CERT: www.us-cert.gov/control_systems/pdf/ICSA-13-016-01.pdf

Arthur Gervais is the CEO of Hatforce, a cybersecurity consultant company in Germany [2]. He has recently disclosed several Schneider Electric vulnerabilities [3] and has posted videos on Youtube, demonstrating attacks on Schneider Electric's Telemecanique line [4].

Sources

[1] http://download.schneider-electric.com/files?p_File_Id=29960974&p_File_Name=SEVD-2013-009-01.pdf
[2] https://www.hatforce.com/
[3] www.us-cert.gov/control_systems/pdf/ICS-ALERT-13-016-01.pdf
[4] http://www.youtube.com/channel/UCZnisJxJCAnfVJHvO1hNmiQ

Schneider Electric – BMX NOE 0110 unauthenticated SOAP/HTTP interface

Versions affected: Unknown

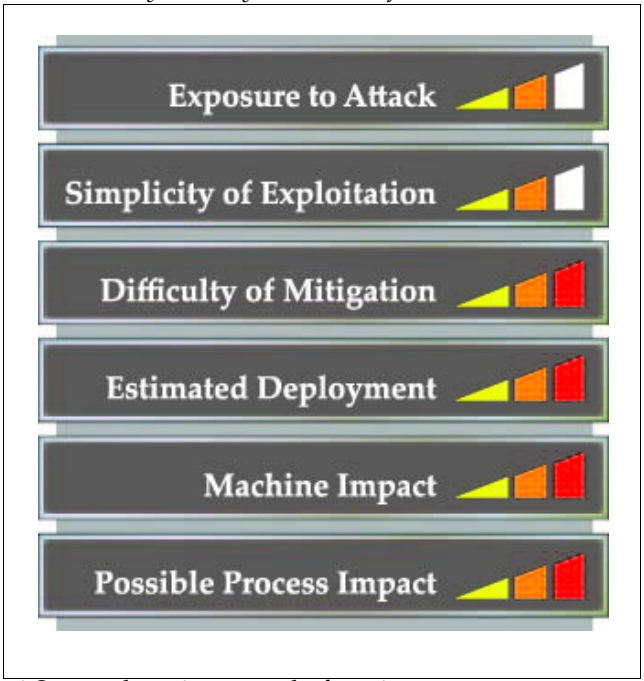
Approximate date public: 1/16/12

Sector primarily affected: Multiple

Description:

Lack of authentication in Schneider Electric's SOAP/HTTP interface allows for arbitrary code execution [1].

Vulnerability Severity Chart (as of 20130113)*



* See explanation at end of section

Exposure to attack: *Medium*

Under recommended practice configuration, the vulnerable system should not be accessible from less-trusted networks.

Simplicity of Exploitation: *Medium*

This vulnerability, along with proof of concept, was presented at Digital Bond's S4 2013 Conference. However exploit code was not made publicly available.

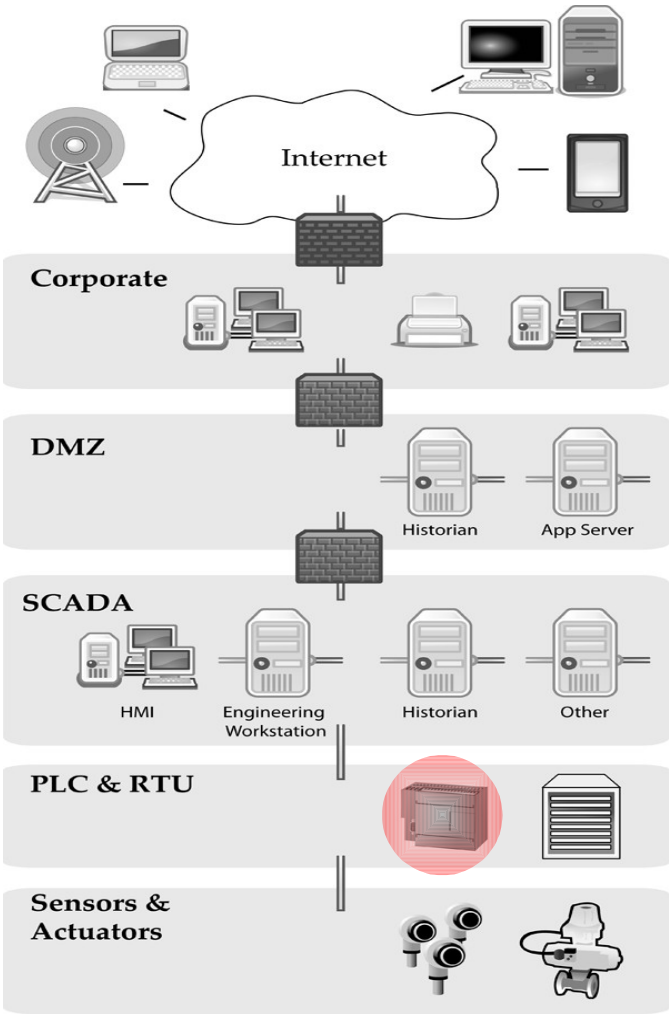
Difficulty of mitigation: *High*

The vendor has not released a patch to address this vulnerability.

Estimated deployment: *High*

Schneider Electric is a world leading automation vendor headquartered in France. The BMX NOE 0110 is an ethernet module used in the Modicon M340 automation platform [2].

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



Machine impact: *High*

Successful exploitation allows for arbitrary code execution.

Possible process impact: *High*

As successful exploitation allows for arbitrary code execution on a PLC, an attacker could leverage this vulnerability to interact with portions of the controlled process at will.

Additional analysis:

Port number (s) of affected service: 80/TCP

This vulnerability was discovered or disclosed by: Arthur Gervais

National Vulnerability Database:

ICS-CERT: www.us-cert.gov/control_systems/pdf/ICS-ALERT-13-016-01.pdf

Arthur Gervais is the CEO of Hatforce, a cybersecurity consultant company in Germany [3]. Gervais disclosed and demonstrated this vulnerability, along with three others also from Schneider Electric, at Digital Bond's S4 Conference in January 2013 [1]. He has also posted videos on Youtube, demonstrating attacks on Schneider Electric's Telemecanique line [4].

Sources

[1] www.us-cert.gov/control_systems/pdf/ICS-ALERT-13-016-01.pdf
[2] http://www2.schneider-electric.com/sites/corporate/en/products-services/automation-control/products-offer/range-presentation.page?c_filepath=/templatedata/Offer_Presentation/3_Range_Datasheet/data/en/shared/automation_and_control/modicon_m340.xml
[3] https://www.hatforce.com/
[4] http://www.youtube.com/channel/UCZnisJxJCAnfVJHvO1hNmiQ

Schneider Electric – Modicon M340 denial of service

Versions affected: Unknown

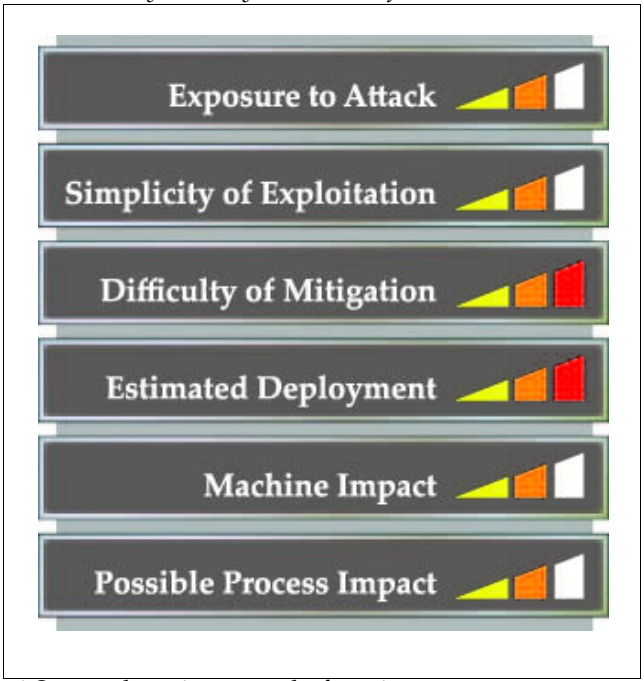
Approximate date public: 1/16/12

Sector primarily affected: Multiple

Description:

Schneider Electric's Modicon M340 is vulnerable to TCP resource exhaustion, which could result in a denial of service [1].

Vulnerability Severity Chart (as of 20130113)*



* See explanation at end of section

Exposure to attack: *Medium*

Under recommended practice configuration, an attacker must have access to the same network segment as the machine running the vulnerable software in order to exploit this vulnerability.

Simplicity of Exploitation: *Medium*

This vulnerability, along with proof of concept, was presented at Digital Bond's S4 2013 Conference. However, the exploit code is not publicly available.

Difficulty of mitigation: *High*

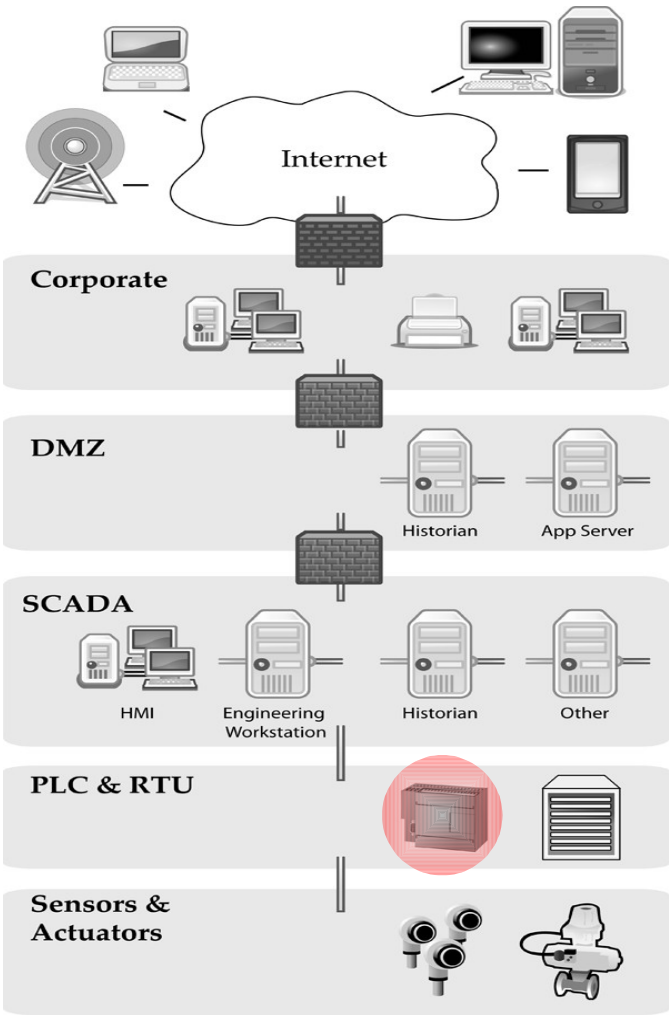
The vendor has not released a patch to address this vulnerability.

Estimated deployment: *High*

Schneider Electric is a world leading automation vendor headquartered in France. Modicon M340 is a programmable logic controller (PLC) that is usually coupled with a programming

software called Utility Pro and is used in several sectors, including: electric, water, and manufacturing [2].

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



Machine impact: *Medium*

Successful exploitation allows for denial of service

Possible process impact: *Medium*

As successful exploitation allows for denial of service on a PLC ethernet module, impact will vary by process.

Additional analysis:

Port number (s) of affected service:

This vulnerability was discovered or disclosed by: Arthur Gervais

National Vulnerability Database:

ICS-CERT: www.us-cert.gov/control_systems/pdf/ICS-ALERT-13-016-01.pdf

Arthur Gervais is the CEO of Hatforce, a cybersecurity consultant company in Germany [3]. Gervais disclosed and demonstrated this vulnerability, along with three others also from Schneider Electric, at Digital Bond's S4 Conference in January 2013 [1]. He has also posted videos on Youtube, demonstrating attacks on Schneider Electric's Telemecanique line [4].

Sources

[1] www.us-cert.gov/control_systems/pdf/ICS-ALERT-13-016-01.pdf
[2] http://www2.schneider-electric.com/sites/corporate/en/products-services/automation-control/products-offer/range-presentation.page?c_filepath=/templatedata/Offer_Presentation/3_Range_Datasheet/data/en/shared/automation_and_control/modicon_m340.xml
[3] https://www.hatforce.com/
[4] http://www.youtube.com/channel/UCZnisJxJCAnfVJHvO1hNmiQ

Schneider Electric – Modicon M340 cross-site scripting

Versions affected: Unknown

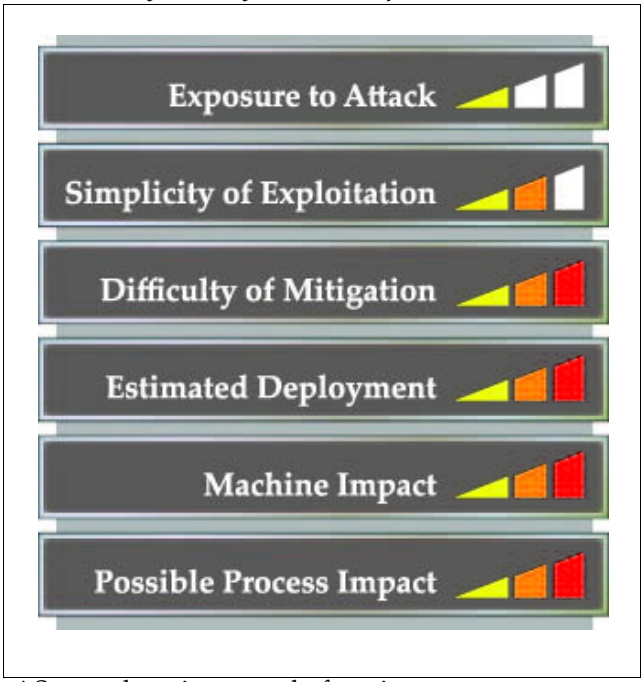
Approximate date public: 1/16/12

Sector primarily affected: Multiple

Description:

Schneider Electric's Modicon M340 is vulnerable to a cross-site scripting vulnerability [1].

Vulnerability Severity Chart (as of 20130113)*



* See explanation at end of section

Exposure to attack: *Low*

Successful exploitation requires user interaction with attacker-controlled resources (visiting a malicious Web page) – hosted on the PLC's embedded Web server.

Simplicity of Exploitation: *Medium*

This vulnerability, along with proof of concept, was presented at Digital Bond's S4 2013 Conference. However, the proof of concept code has not been made public.

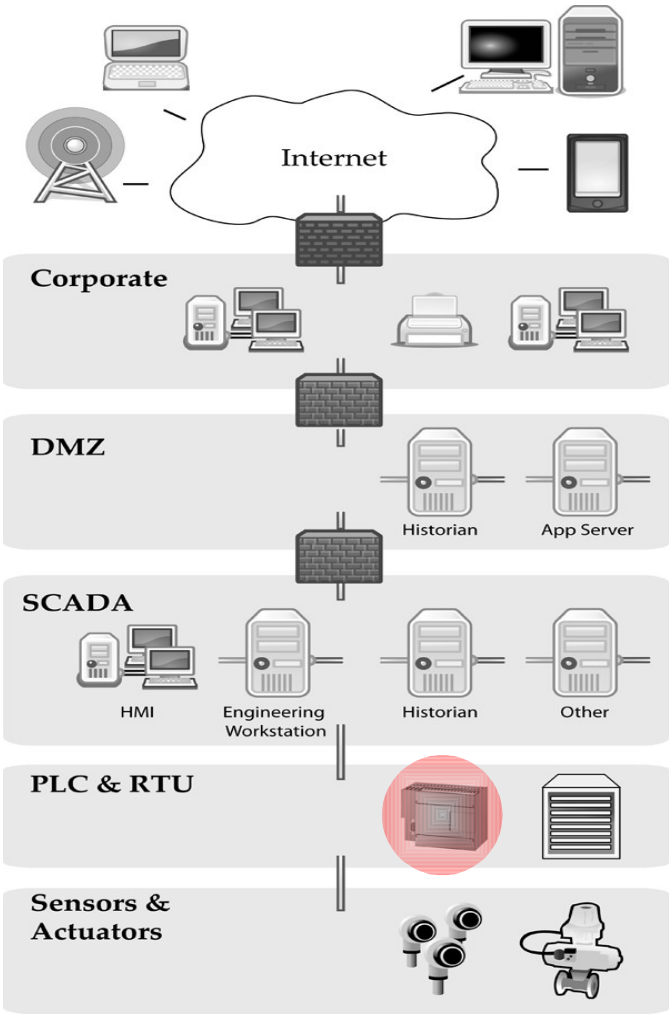
Difficulty of mitigation: *High*

The vendor has not released a patch to address this vulnerability.

Estimated deployment: *High*

Schneider Electric is a world leading automation vendor headquartered in France. Modicon M340 is a programmable logic controller (PLC) that is used in several sectors, including: electric, water, and manufacturing [2].

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



Machine impact: *High*

This vulnerability allows an attacker to issue specific commands to a PLC.

Possible process impact: *High*

Successful exploitation of this vulnerability potentially allows the attacker to interact with the process at will.

Additional analysis:

Port number (s) of affected service: 80

This vulnerability was discovered or disclosed by: Arthur Gervais

National Vulnerability Database:

ICS-CERT: www.us-cert.gov/control_systems/pdf/ICS-ALERT-13-016-01.pdf

Arthur Gervais is the CEO of Hatforce, a cybersecurity consultant company in Germany [3]. Gervais disclosed and demonstrated this vulnerability, along with three others also from Schneider Electric, at Digital Bond's S4 Conference in January 2013 [1]. He has also posted videos on Youtube, demonstrating attacks on Schneider Electric's Telemecanique line [4].

Sources

[1] www.us-cert.gov/control_systems/pdf/ICS-ALERT-13-016-01.pdf
[2] http://www2.schneider-electric.com/sites/corporate/en/products-services/automation-control/products-offer/range-presentation.page?c_filepath=/templatedata/Offer_Presentation/3_Range_Datasheet/data/en/shared/automation_and_control/modicon_m340.xml
[3] https://www.hatforce.com/
[4] http://www.youtube.com/channel/UCZnisJxJCAnfVJHvO1hNmiQ

Schneider Electric – Magelis XBT hard-coded credentials

Versions affected: Unknown

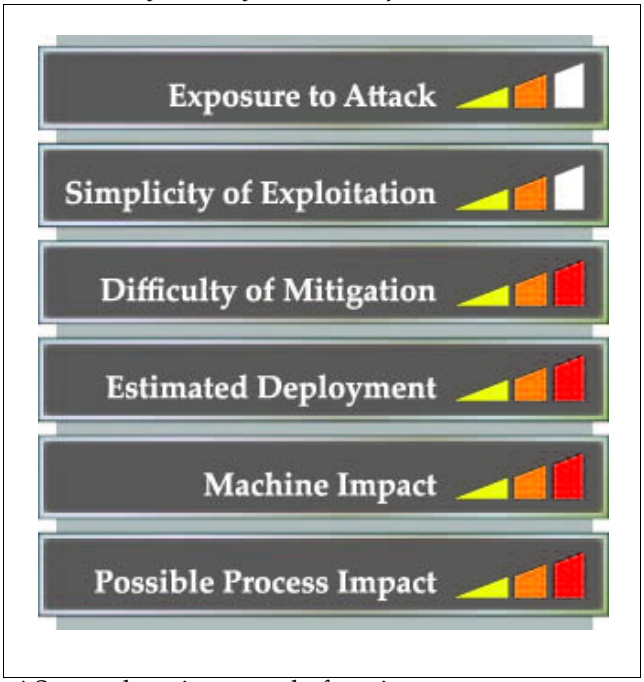
Approximate date public: 1/16/12

Sector primarily affected: Multiple

Description:

Schneider Electric's Magelis XBT has hard-coded credentials [1].

Vulnerability Severity Chart (as of 20130113)*



* See explanation at end of section

Exposure to attack: *Medium*

Successful exploitation requires access to the same network segment as the vulnerable device.

Simplicity of Exploitation: *Medium*

This vulnerability, along with proof of concept, was presented at Digital Bond's S4 2013 Conference. However, the proof of concept code has not been made public.

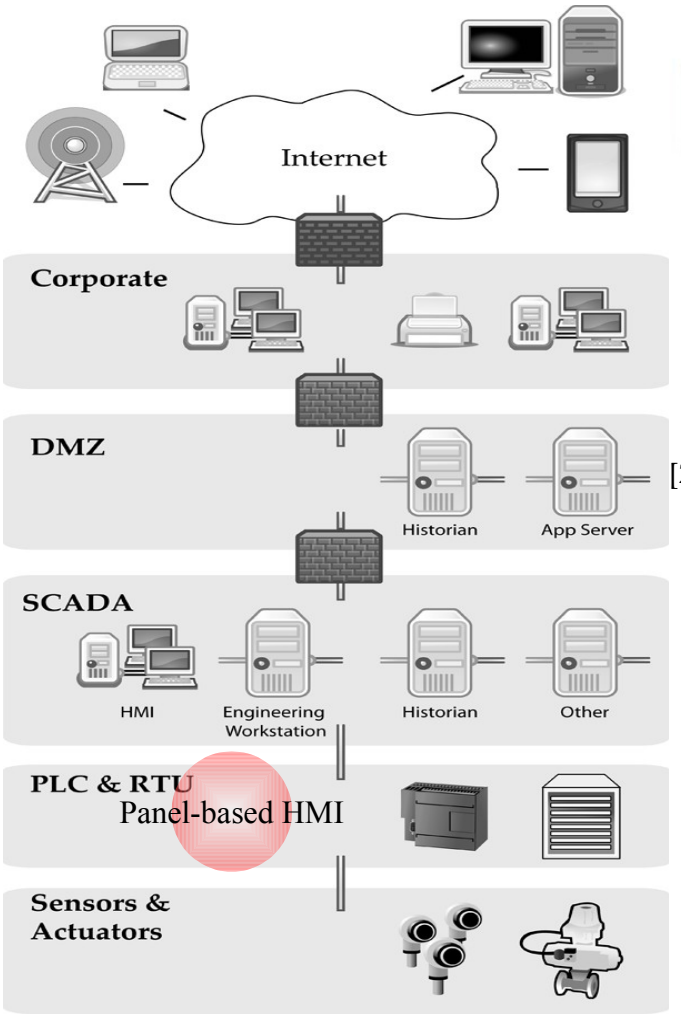
Difficulty of mitigation: *High*

The vendor has not released a patch to address this vulnerability.

Estimated deployment: *High*

Schneider Electric is a world leading automation vendor headquartered in France. The Maglelis XBT are a series of advanced touchscreen panels used in building automation and manufacturing [2].

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



[2]

Machine impact: *High*

Successful exploitation allows users to log-on to the affected device.

Possible process impact: *High*

As successful exploitation allows for attacker to control an HMI device, process impact is high.

Additional analysis:

Port number (s) of affected service: 6001/TCP

This vulnerability was discovered or disclosed by: Arthur Gervais

National Vulnerability Database:

ICS-CERT: www.us-cert.gov/control_systems/pdf/ICS-ALERT-13-016-01.pdf

Arthur Gervais is the CEO of Hatforce, a cybersecurity consultant company in Germany [3]. Gervais disclosed and demonstrated this vulnerability, along with three others also from Schneider Electric, at Digital Bond's S4 Conference in January 2013 [1]. He has also posted videos on Youtube, demonstrating attacks on Schneider Electric's Telemecanique line [4].

Sources

[1] http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-13-016-01.pdf
[2] http://www2.schneider-electric.com/sites/corporate/en/products-services/automation-control/products-offer/range-presentation.page?c_filepath=/templatedata/Offer_Presentation/3_Range_Datasheet/data/en/shared/automation_and_control/magelis_xbt_gt.xml#
[3] https://www.hatforce.com/
[4] http://www.youtube.com/channel/UCZnisJxJCAnfVJHvO1hNmiQ

Siemens – SIMATIC RF Manager buffer overflow

Versions affected: RF-MANAGER 2008
RF-MANAGER Basic v3.0 and lower (as distributed with RF670R and RF640R)

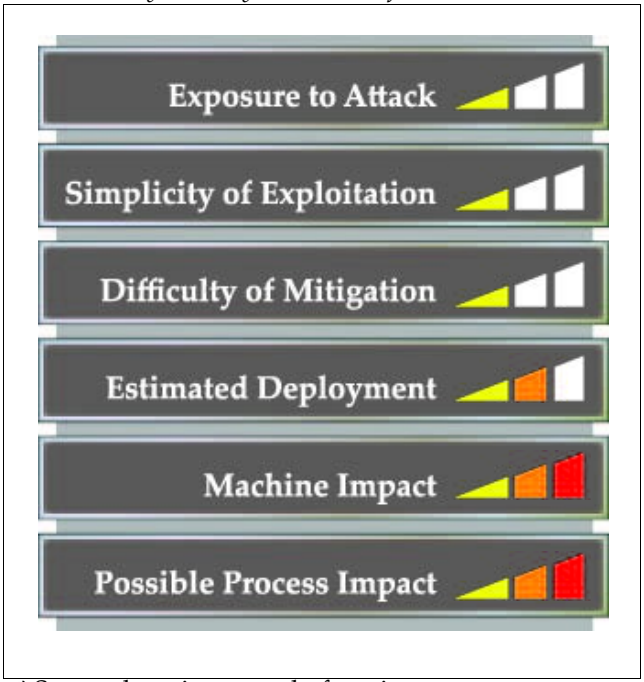
Approximate date public: 1/11/13

Sector primarily affected: Multiple

Description:

A buffer overflow in an ActiveX component can lead to remote code execution in the context of the browser. Depending on the configuration of the affected system, this may be the privileged administrator user. As it is recommended not to use the administrative account for daily work, it is assumed that unprivileged user is affected. [1]

Vulnerability Severity Chart (as of 20130113)*



* See explanation at end of section

Exposure to attack: *Low*

Successful exploitation requires user interaction with attacker-controlled resources (visiting a malicious Web page).

Simplicity of Exploitation: *Low*

Details concerning this vulnerability are limited.

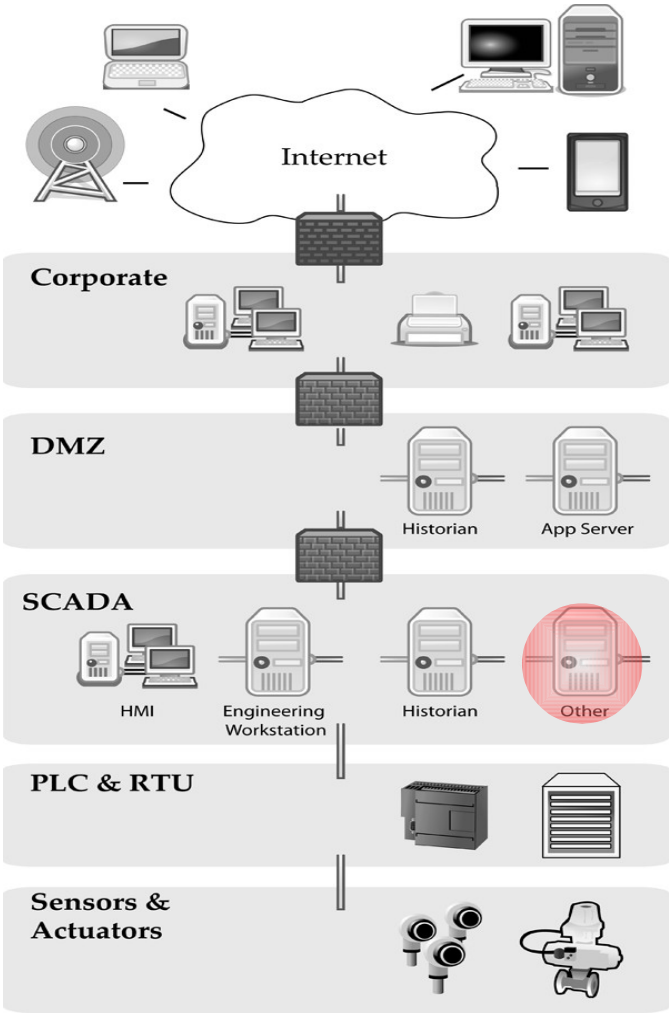
Difficulty of mitigation: *Low*

The vendor has released a patch to address this vulnerability. The patch can obtained via customer support [1].

Estimated deployment: *Medium*

Siemens is a world leading industrial and automation company based in Germany. SIMATIC RF Manager "is an engineering and configuration tool for RFID readers like Simatic RF600 from lower layers up to ERP layer and MES layer" [1].

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



Machine impact: *High*

Successful exploitation allows for arbitrary code execution the browser and could result in full

system control [1].

Possible process impact: *High*

As successful exploitation allows for arbitrary code execution the browser, impact will vary by process.

Additional analysis:

Port number (s) of affected service: 80

This vulnerability was discovered or disclosed by:

National Vulnerability Database:

ICS-CERT: www.us-cert.gov/control_systems/pdf/ICSA-13-014-01.pdf

Sources

[1] www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-099741.pdf

Smart Software Solutions – CoDeSys weak access control update

Versions affected: Version 2.3.X and 2.4.X

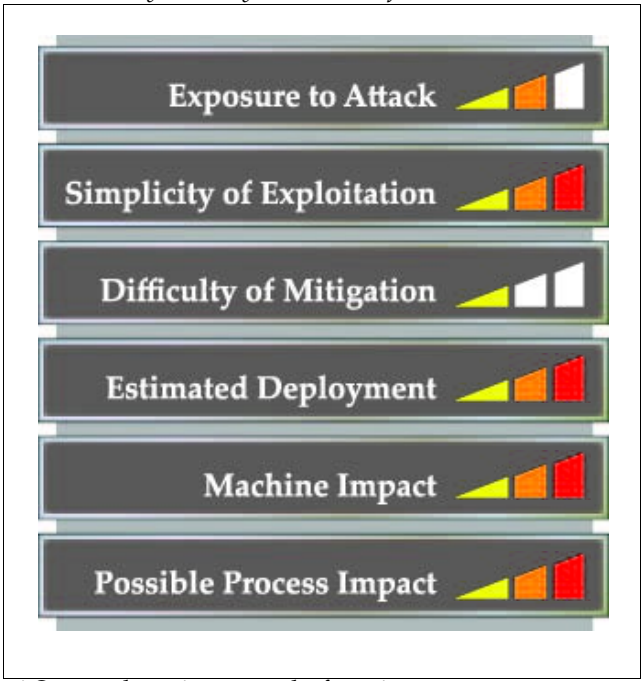
Approximate date public: April 6, 2012

Sector primarily affected: Multiple

Description:

CoDeSys ladder logic runtime uses weak access control (for uploading communication with the PLC) [1]. In essence, the cyclical redundancy check (CRC) can be bypassed.

Vulnerability Severity Chart (as of 20130113)*



* See explanation at end of section

Exposure to attack: *Medium*

Under recommended practice, the vulnerable software is not accessible from less trusted networks.

Simplicity of Exploitation: *High*

Digital Bond's Project Basecamp has developed attack tools to exploit this vulnerability: codesys-shell.py and codesys-transfer.py. The codesys-shell.py allows an attacker to access "the CoDeSys command shell without authentication" and the codesys-transfer.py allows an attacker to "read or write files to the PLC without authentication" [6-7]. These tools "can easily be ported to be Metasploit modules, and could be made to run the Meterpreter shell on supported operating systems" [7].

Difficulty of mitigation: *Low*

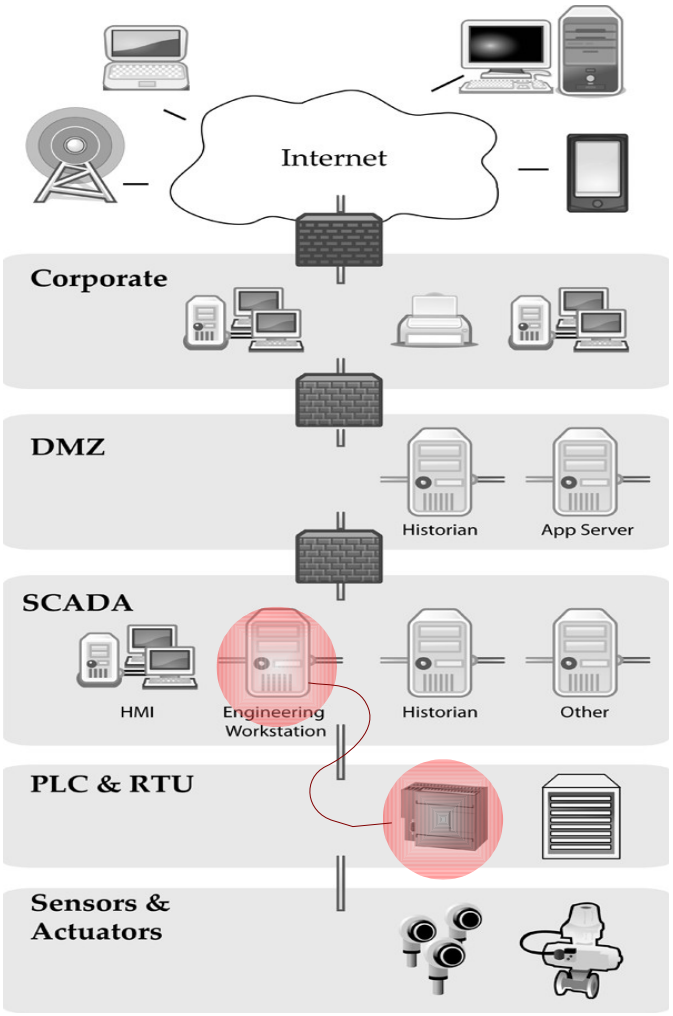
The vendor has released a patch to address this vulnerability [9]. The patch can be

downloaded via the CoDeSys website [10].

Estimated deployment: *High*

Smart Software Solutions (3S) is a German-based software company whose principal product is the CoDeSys development environment. CoDeSys is an acronym standing for controller development system which implements the IEC 61161-3 standard describing programming languages used in programmable logic controllers (PLCs) including: function block diagram, structured list, instruction list, and sequential function chart [2]. The CoDeSys system is OEMed by a variety of other automation companies, including ABB, Beckhoff, Kontron, Schneider Electric, Schweitzer Engineering Laboratory, and WAGO [3]. CoDeSys is installed on hundreds of thousands of devices throughout the world [4]. CoDeSys user base is concentrated in Europe [5]. At least 261 vendors, that use the CoDeSys latter logic, could be vulnerable to this exploit [8].

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



Machine impact: *High*

Successful exploitation allows for privilege escalation, in some cases allowing for execution of arbitrary code.

Possible process impact: *High*

As successful exploitation allows for arbitrary code execution on an controller machine, an attacker could leverage this vulnerability to interact with a portion of the controlled process at will.

Additional analysis:

Port number (s) of affected service:

This vulnerability was discovered or disclosed by: Reid Wightman

National Vulnerability Database:

ICS-CERT: www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-097-02.pdf
www.us-cert.gov/control_systems/pdf/ICSA-13-011-01.pdf

This vulnerability was presented by Reid Wightman of Digital Bond at the OWASP Appsec DC security conference [1].
This vulnerability was previously reported in the 20120408 and 20121021 Weekly Report.

Sources

[1] http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-097-02.pdf
[2] http://www.3s-software.com/index.shtml?WebVisu_en
[3] http://www.3s-software.com/index.shtml?homepage
[4] http://www.3s-software.com/index.shtml?en_sp4
[5] http://www.users-conference.com/
[6] http://www.digitalbond.com/2012/10/25/new-project-basecamp-tools-for-codesys-200-vendors-affected/
[7] http://www.digitalbond.com/tools/basecamp/3s-codesys/
[8] http://www.3s-software.com/index.shtml?en_Company_ref
[9] www.us-cert.gov/control_systems/pdf/ICSA-13-011-01.pdf
[10] http://www.codesys.com/download.html

SpecView – SpecView Web Server directory traversal update

Versions affected: 2.5 build 853 and previous

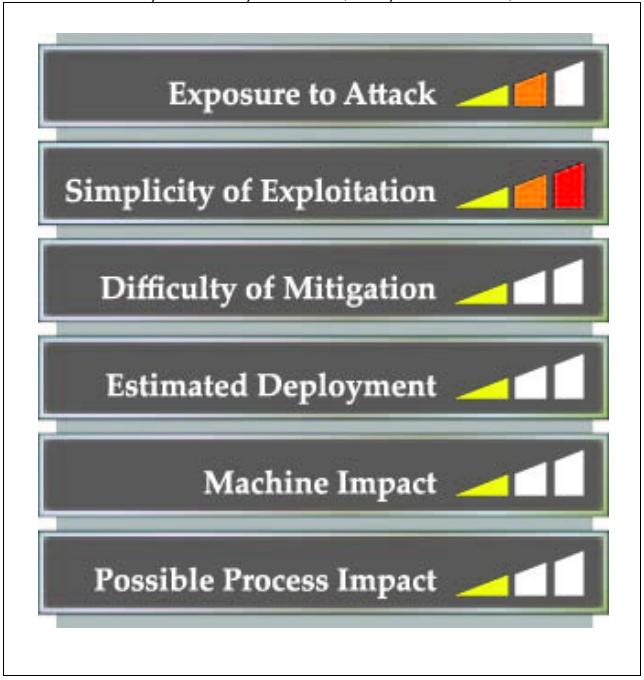
Approximate date public: 6/29/12

Sector primarily affected: Multiple

Description:

The Web server used by SpecView is vulnerable to directory traversal.

Vulnerability Severity Chart (as of 20130113)*



* See explanation at end of section

Exposure to attack: *Medium*

Under recommended practice, the vulnerable software is not accessible from less trusted networks.

Simplicity of Exploitation: *High*

Exploit code is publicly available:
http://SERVER/.../.../.../.../.../boot.ini
http://SERVER/...\...\...\...\...\...\boot.ini
[1].

Difficulty of mitigation: *Low*

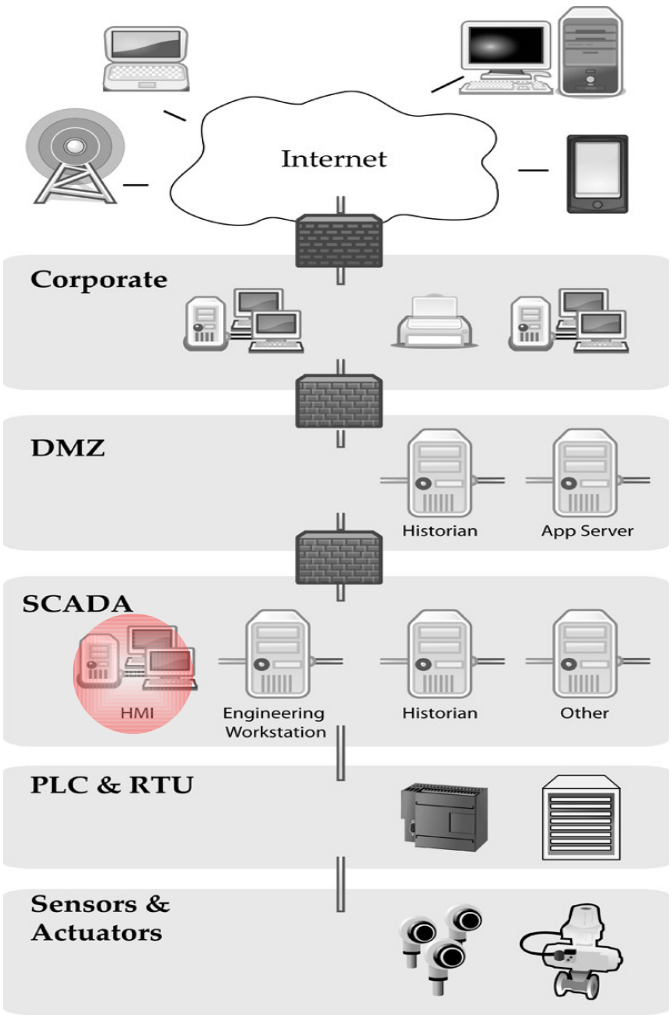
The vendor has released a patch to address this vulnerability [8].

Estimated deployment: *Low*

SpecView is a SCADA software company headquartered in the U.K. [2]. Details on deployments are largely unknown, though the software does appear to have a user manual in several languages [3], and several Web sites describe and offer to sell the software [4-7]. SpecView appears to be deployed several sectors, including: food processing and

manufacturing [9].

The following diagram shows where the vulnerable software would reside (highlighted in red) in a simplified network diagram based on the ISA 99 reference architecture.



Machine impact: *Low*

Successful exploitation allows for information gain.

Possible process impact: *Low*

Information gained through this attack could be used in other attacks.

Additional analysis:

Port number (s) of affected service: 80

This vulnerability was discovered or disclosed by: Luigi Auriemma

National Vulnerability Database:

ICS-CERT: www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-214-01.pdf
www.us-cert.gov/control_systems/pdf/ICSA-13-011-02.pdf

Sources

[1] http://aluigi.altervista.org/adv/specview_1-adv.txt
[2] http://www.specview.com/html/contact_us.html
[3] ftp://62.49.124.34/Manual/
[4] http://www.cascade.net/index.php?q=node/340
[5] http://www.entherm.com/SpecView-Mfg%20Page.html
[6] http://www.honeywell.sk/?com=documents&id=557
[7] http://www.dmgcsl.co.uk/services/plc.htm
[8] http://www.specview.com/html/downloads.html
[9] http://www.specview.com/html/applications.html

Explanation of Vulnerability Severity Chart

The Vulnerability Severity Chart is intended to depict the general severity of a vulnerability at a glance. The chart ranks six vulnerability characteristics qualitatively as high, medium, or low as of the date listed. The rankings are subject to change as the situation develops. Description of the characteristics and ranking criteria are provided below.

Characteristic	Description
Exposure to attack High Medium Low	What privileges and location are necessary for successful attack? Exploitable from a less trusted network without authentication Presence on same network segment or authentication required Access to local machine or user complicity required
Simplicity of exploitation High Medium Low	How simple is it to launch a successful attack against the vulnerability? Exploit module publicly available Technical detail available No technical detail available
Difficulty of Mitigation High Medium Low	How easily can the vulnerability be mitigated? No patch available Workaround only or firmware update required Patch available
Estimated Deployment High Medium Low	In the sector of greatest deployment, what is the estimated market share? Greater than 25% 10% to 25% Less than 10%
Machine Impact High Medium Low	What level of control does successful exploitation give the attacker? Full machine control (arbitrary code execution) Denial of service or privilege escalation Information gain
Possible Process Impact High Medium Low	How much damage could an attacker do given successful exploitation of the vulnerability? Substantial damage and/or loss of life Moderate damage No damage

Vulnerabilities that Potentially Affect ICS

The US-CERT Weekly Vulnerability Bulletin included information on 71 vulnerabilities. Of these, 11 are for products commonly deployed in control system networks. This list does not include vulnerabilities that require user interaction with attacker-controlled resources; vulnerabilities in office applications and Web browsers are excluded. Vulnerabilities are grouped by high, medium, and low severity based on Common Vulnerability Scoring System (CVSS) scores.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- java	Unspecified vulnerability in the JRE component in IBM Java 7 SR2 and earlier, Java 6.0.1 SR3 and earlier, Java 6 SR11 and earlier, Java 5 SR14 and earlier, and Java 142 SR13 FP13 and earlier; as used in IBM Rational Host On-Demand, Rational Change, Tivoli Monitoring, Smart Analytics System 5600, Tivoli Remote Control 5.1.2, WebSphere Real Time, Lotus Notes & Domino, Tivoli Storage Productivity Center, and Service Deliver Manager; and other products from other vendors such as Red Hat, when running under a security manager, allows remote attackers to gain privileges by modifying or removing the security manager via vectors related to "insecure use of the java.lang.reflect.Method invoke() method."	2013-01-10	9.3	CVE-2012-4820
ibm -- java	Multiple unspecified vulnerabilities in the JRE component in IBM Java 7 SR2 and earlier, Java 6.0.1 SR3 and earlier, Java 6 SR11 and earlier, Java 5 SR14 and earlier, and Java 142 SR13 FP13 and earlier; as used in IBM Rational Host On-Demand, Rational Change,	2013-01-10	9.3	CVE-2012-4821

	Tivoli Monitoring, Smart Analytics System 5600, Tivoli Remote Control 5.1.2, WebSphere Real Time, Lotus Notes & Domino, Tivoli Storage Productivity Center, and Service Deliver Manager; and other products from other vendors such as Red Hat, allow remote attackers to execute arbitrary code via "insecure use" of the (1) java.lang.Class getDeclaredMethods or nd (2) java.lang.reflect.AccessibleObject setAccessible() methods.			
ibm -- java	Multiple unspecified vulnerabilities in the JRE component in IBM Java 7 SR2 and earlier, Java 6.0.1 SR3 and earlier, Java 6 SR11 and earlier, Java 5 SR14 and earlier, and Java 142 SR13 FP13 and earlier; as used in IBM Rational Host On-Demand, Rational Change, Tivoli Monitoring, Smart Analytics System 5600, Tivoli Remote Control 5.1.2, WebSphere Real Time, Lotus Notes & Domino, Tivoli Storage Productivity Center, and Service Deliver Manager; and other products from other vendors such as Red Hat, allow remote attackers to execute arbitrary code via vectors related to "insecure use [of] multiple methods in the java.lang.class class."	2013-01-10	9.3	CVE-2012-4822
ibm -- java	Unspecified vulnerability in the JRE component in IBM Java 7 SR2 and earlier, Java 6.0.1 SR3 and earlier, Java 6 SR11 and earlier, Java 5 SR14 and earlier, and Java 142 SR13 FP13 and earlier; as used in IBM Rational Host On-Demand, Rational Change, Tivoli Monitoring, Smart Analytics System 5600, Tivoli Remote Control 5.1.2, WebSphere Real Time, Lotus Notes & Domino, Tivoli Storage Productivity	2013-01-10	9.3	CVE-2012-4823

	Center, and Service Deliver Manager; and other products from other vendors such as Red Hat, allows remote attackers to execute arbitrary code via vectors related to "insecure use of the java.lang.ClassLoder defineClass() method."			
microsoft -- windows_7	The Print Spooler in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted print job, aka "Windows Print Spooler Components Vulnerability."	2013-01-09	10.0	CVE-2013-0011
oracle -- jdk	The MBeanInstantiator in Oracle Java Runtime Environment (JRE) 1.7 in Java 7 Update 10 and earlier allows remote attackers to execute arbitrary code via vectors related to unspecified classes that allow access to the class loader, as exploited in the wild in January 2013, as demonstrated by Blackhole and Nuclear Pack, and a different vulnerability than CVE-2012-4681.	2013-01-10	10.0	CVE-2013-0422

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_7	win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle window broadcast messages, which allows local users to gain privileges via a crafted application, aka "Win32k Improper Message Handling	2013-01-09	6.9	CVE-2013-0008

	Vulnerability."			
microsoft -- windows_7	The SSL provider component in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle encrypted packets, which allows man-in-the-middle attackers to conduct SSLv2 downgrade attacks against (1) SSLv3 sessions or (2) TLS sessions by intercepting handshakes and injecting content, aka "Microsoft SSL Version 3 and TLS Protocol Security Feature Bypass Vulnerability."	2013-01-09	5.8	CVE-2013-0013
redhat -- certificate_system	Multiple cross-site scripting (XSS) vulnerabilities in Red Hat Certificate System (RHCS) before 8.1.3 allow remote attackers to inject arbitrary web script or HTML via the (1) pageStart or (2) pageSize to the displayCRL script, or (3) nonce variable to the profileProcess script.	2013-01-04	4.3	CVE-2012-4543
redhat -- certificate_system	The token processing system (pki-tps) in Red Hat Certificate System (RHCS) before 8.1.3 does not properly handle interruptions of token format operations, which allows remote attackers to cause a denial of service (NULL pointer dereference and Apache httpd web server child process crash) via unspecified vectors.	2013-01-04	4.0	CVE-2012-4555
redhat -- certificate_system	The token processing system (pki-tps) in Red Hat Certificate System (RHCS) before 8.1.3 allows remote attackers to cause a denial of service (Apache httpd web server child process restart) via certain unspecified empty search fields in a user certificate search query.	2013-01-04	4.0	CVE-2012-4556

Attack Tools that Potentially Affect ICS

This section describes attack tools that potentially affect control systems that were identified during the reporting period.

Tool name:	**WinCC Harvester**
Date identified:	November 7, 2012
Tool availability:	Open Source [1-2]
Description:	WinCC Harvester is a Metasploit module that uses *"WinCC MS SQL access to harvest sensitive information (users, roles, PLCs) from the database" [3].*
Analysis:	WinCC Harvester is a Metasploit module developed by Positive Technologies, also known as SCADA StrangeLove [1]. As noted in the description, the tool is used to collect sensitive information from WinCC's database that relies on Microsoft SQL. Possible information that can be gathered includes: users, roles, and PLCs [1]. It appears as though the tool is intended for post-incident analysis, as SCADA StrangeLove described the tool as a "Metasploit module for Siemens SIMATIC WinCC forensic/postexploitation" [1]; however, Critical Intelligence points out that the tool, like many security tools, could be used for offensive purposes as well. SCADA StrangeLove posted brief instructions on how to install and initialize the tool: *Copy this file to: /opt/metasploit/msf3/modules/auxiliary/admin/scada/* *Use: use auxiliary/admin/scada/wincc_harvester [1-2]* SCADA StrangeLove has mentioned the tool at the Chaos Communication Congress [6 (Slide 54)] and Power of Community [7] cybersecurity conferences.
Sources:	[1] http://scadastrangelove.blogspot.com/2012/11/wincc-harvester.html [2] https://github.com/nxnrt/wincc_harvester [3] http://www.digitalbond.com/blog/2012/11/09/friday-news-notes-53/ [4] http://scadastrangelove.blogspot.ru/2012/12/siemens-simatic-wincc-7x-security.html [5] http://www.slideshare.net/qqlan/positive-technologies-wincc-security-hardening-guide [6] http://scadastrangelove.blogspot.com/2012/12/scada-strangelove-29c3.html [7] http://ptsecurity.com/about/news/13472/

Tool name:	**ProFuzz**
Date identified:	December 2012
Tool availability:	Open Source [1]
Description:	*Simple PROFINET fuzzer based on Scapy... [1]*
Analysis:	ProFuzz is a python script based on the packet manipulation program, Scapy [2], that allows "the fuzzing of some PROFINET frames" [1] – which means the tool could be used to find security bugs. Profinet is a communications protocol used for real time communications over Ethernet [3]; and is used most frequently by automation products from Siemens [4]. It was created by Dmitrijs Solovjovs, Tobias Leitenmaier, and Daniel Mayer as a student project at the University of Applied Sciences Augsburg, Germany. The tool implements the following PROFINET frames: • *afr (Alarm Frame Random)* • *afo (Alarm Frames Ordered)* • *pnio (Cyclic RealTime)* • *dcp (DCP Identity Requests)* • *ptcp (Precision Transparent Clock Protocol – BETA) [1]* An example and tutorial for running the tool was also included in the README.md file: *sudo python Fuzzer.py -w false -s 00:19:99:9d:ed:ab -d 00:1b:1b:17:ba:8a -t dcp -i eth2 -c 100* **Explanation** • *-s -> Source MAC* • *-d -> Destination MAC* • *-t one of the scan types mentioned above* • *-i, "--interface" -> Interface from which to send. For Example: eth0* • *-c, "--count" -> number of Frames to send*

	• *-w,"--sniff" -> use sniffing(true or false) (should be false)*
Sources:	[1] https://github.com/HSASec/ProFuzz#readme [2] http://www.secdev.org/projects/scapy/ [3] http://www.profibus.com/technology/profinet/overview/ [4] http://www.automation.siemens.com/mcms/automation/en/industrial-communications/profinet/pages/default.aspx

ICS Network Activity

This section presents network port activity for commonly used control system ports. This activity may represent legitimate control systems traffic. It may also represent other traffic using these ports. Spikes in targets may represent attempts to locate or attack services using these ports. Spikes in sources may represent distributed scanning. Spikes in records may represent repeated connection attempts. Analysis is based on data provided by the SANS Internet Storm Center.

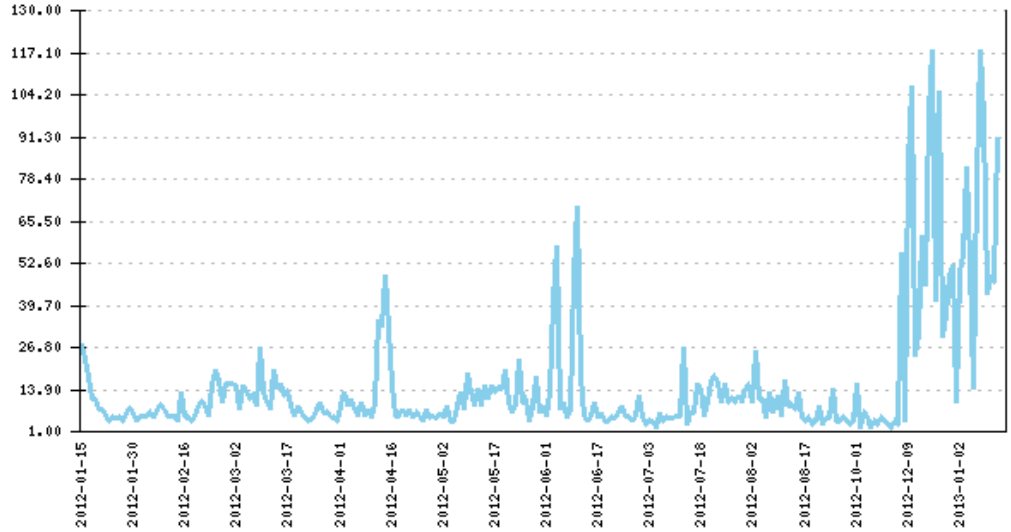
Critical Intelligence monitors 245 control system related ports. Of these, 7 ports recorded spikes that were highly significant (two standard deviations from the mean or above 95% of reported 12 month activity).

Highly Significant Spikes

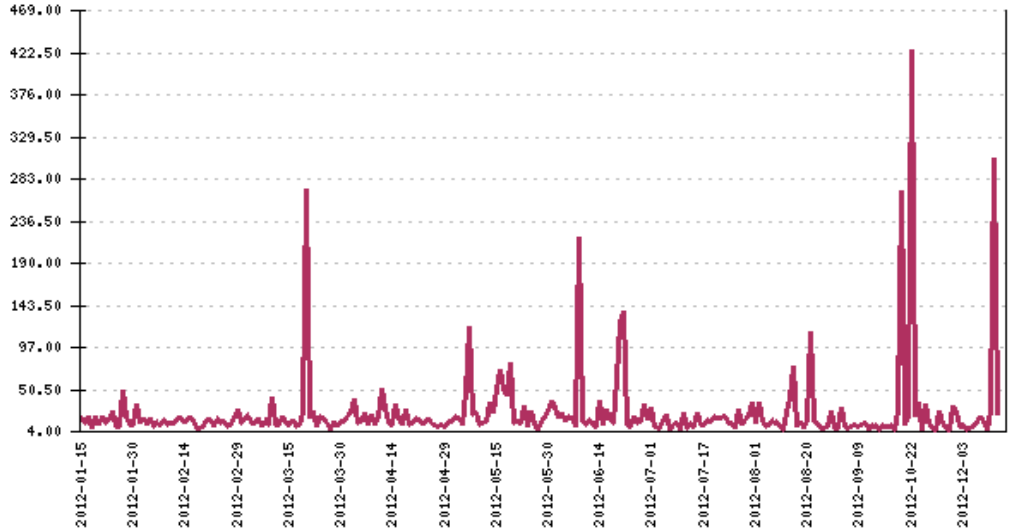
- Port 502: Spike in targets Jan 08 - Modbus TCP

Note: These recent spikes indicate that someone may be scanning for modbus/TCP devices connected directly to the Internet.

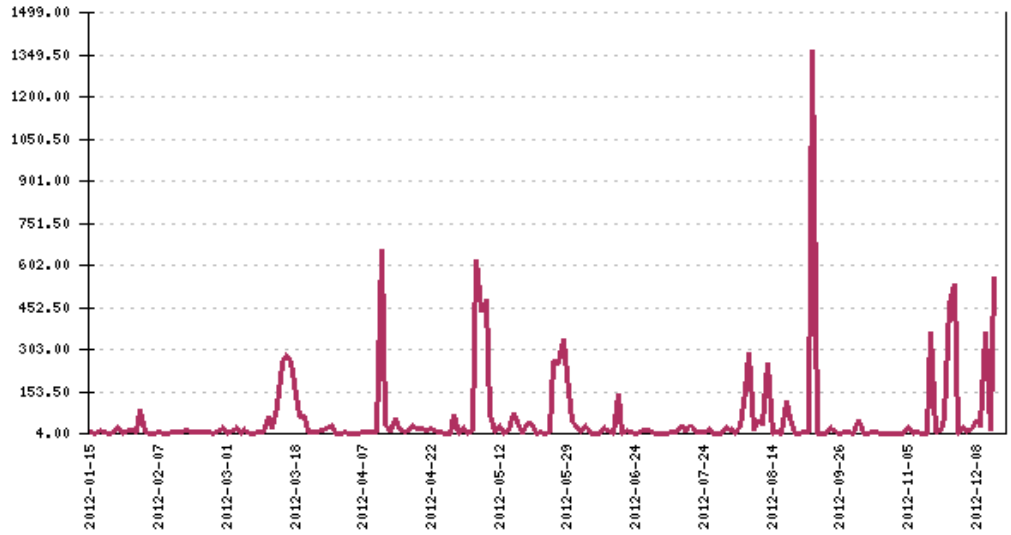
- Port 13782: Spike in records Jan 11 - ABB Ranger 2003
- Port 45678: Spike in records & targets Jan 09 - Foxboro/Invensys Foxboro DCS AIMAPI
- Port 56002: Spike in records Jan 08 - Telvent OASyS DNA
- Port 56014: Spike in records Jan 11 - Telvent OASyS DNA
- Port 56015: Spike in records Jan 12 - Telvent OASyS DNA
- Port 56030: Spike in records Jan 09 - Telvent OASyS DNA



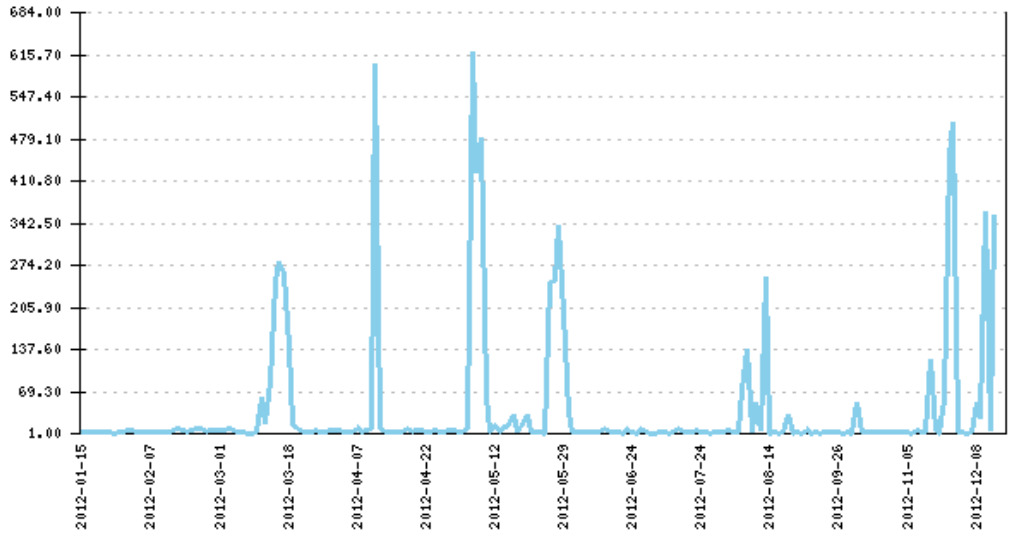
Port 502, potentially used with Modbus TCP, had a spike in targets with 118 reported Jan 08. This is 5.04 standard deviations from the mean of 15.47.



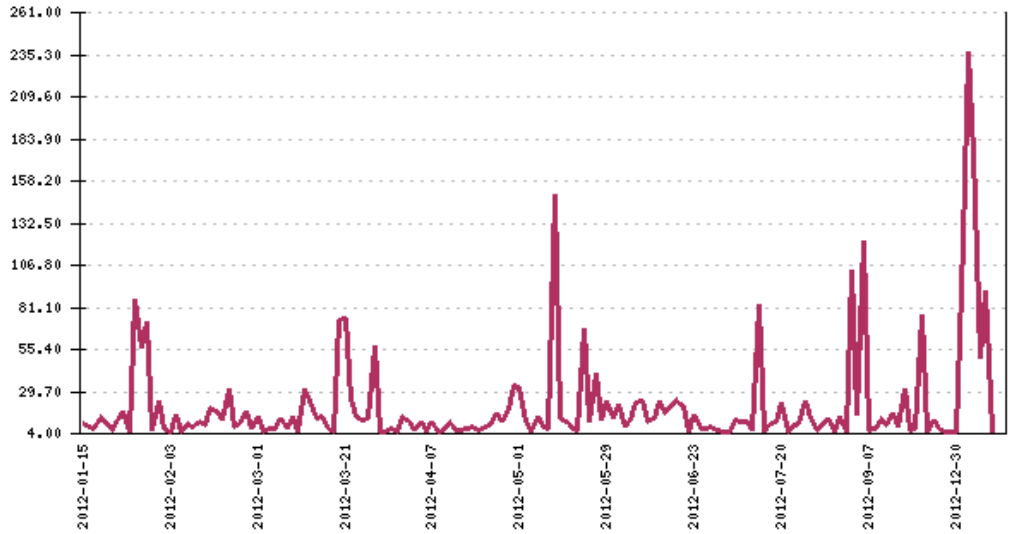
Port 13782, potentially used with ABB Ranger 2003, had a spike in records with 306 reported Jan 11. This is 6.58 standard deviations from the mean of 24.71.



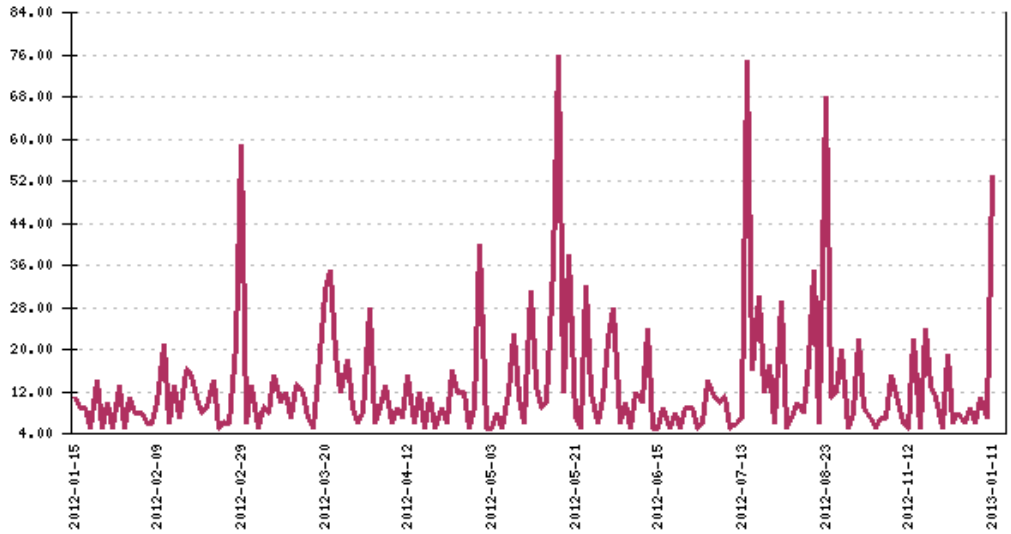
Port 45678, potentially used with Foxboro/Invensys Foxboro DCS AIMAPI, had a spike in records with 557 reported Jan 09. This is 3.38 standard deviations from the mean of 58.9.



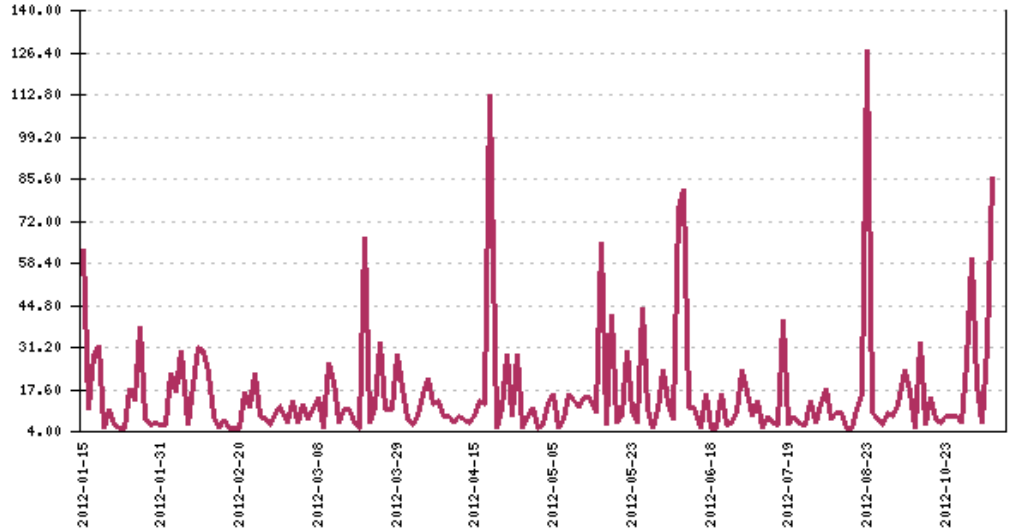
Port 45678, potentially used with Foxboro/Invensys Foxboro DCS AIMAPI, had a spike in targets with 356 reported Jan 09. This is 3.01 standard deviations from the mean of 38.6.



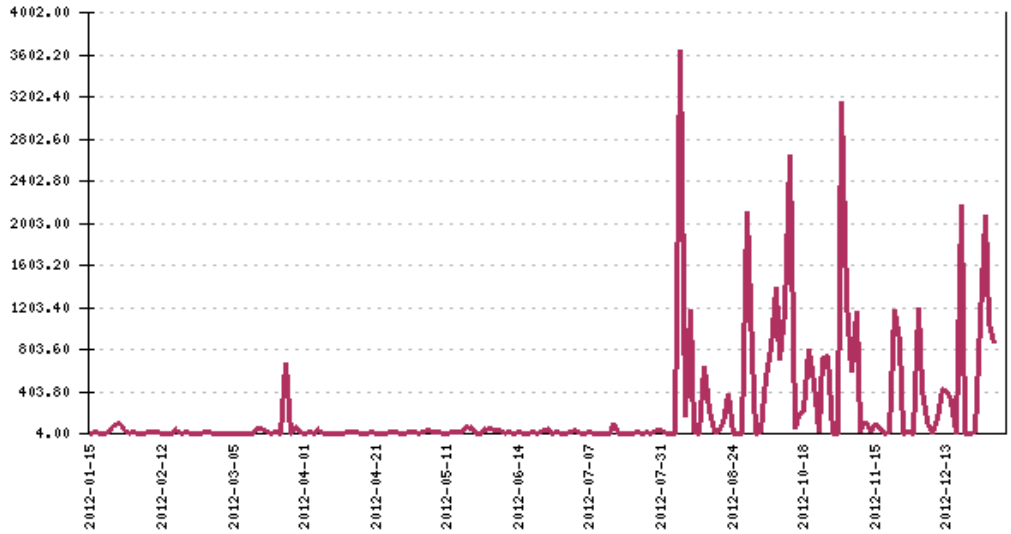
Port 56002, potentially used with Telvent OASyS DNA, had a spike in records with 91 reported Jan 08. This is 2.16 standard deviations from the mean of 21.2.



Port 56014, potentially used with Telvent OASyS DNA, had a spike in records with 53 reported Jan 11. This is 3.29 standard deviations from the mean of 13.16.



Port 56015, potentially used with Telvent OASyS DNA, had a spike in records with 86 reported Jan 12. This is 3.85 standard deviations from the mean of 16.28.



Port 56030, potentially used with Telvent OASyS DNA, had a spike in records with 2079 reported Jan 09. This is 3.46 standard deviations from the mean of 217.66.

Daily and Weekly Network Activity Diagrams are available online.
** Note, the weekly network diagrams are large image file and are best viewed when downloaded and viewed outside the Web browser.*

Weekly list of IP addresses scanning control system ports is available online.

Register for a one-month trial subscription of this weekly NexDefense intelligence report.

Please contact Michael Radigan or visit www.nexdefense.com

Michael Radigan | NexDefense | 614-942-0919
michael.radigan@nexdefense.com