ISRCS 2009

Tutorial

Session 2c: Known ICS Vulnerabilities

Sean McBride, MA
Critical Intelligence

August 11, 2009
Idaho Falls, Idaho

Outline

ISRCS 2009

- What ICS vulnerabilities do we know about?
  - NVD
  - OSVDB
  - Security vendors
  - ICS vendors
- Issues in public disclosure of vulnerability info
  - Code re-use
  - Protection

NVD

ISRCS 2009

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

38079 CVE Vulnerabilities
128 Checklists
178 US-CERT Alerts
2344 US-CERT Vuln Notes
2517 OVAL Queries
17819 CPE Names

Search Results (Refine Search)

There are **4** matching records. Displaying matches **1** through **4**.

CVE-2009-2152

Summary: SQL injection vulnerability in a_index.php in AdaptWeb 0.9.2 allows remote attackers to execute arbitrary SQL commands via the CodigoDisciplina parameter in a TopicosCadastro1 action.

Published: 06/22/2009

CVSS Severity: 7.5 (HIGH)

CVE-2008-5848

Summary: The Advantech ADAM-6000 module has 00000000 as its default password, which makes it easier for remote attackers to obtain access through an HTTP session, and (1) monitor or (2) control the module's Modbus/TCP I/O activity.

Published: 01/06/2009

CVSS Severity: 10.0 (HIGH)

CVE-2008-2639

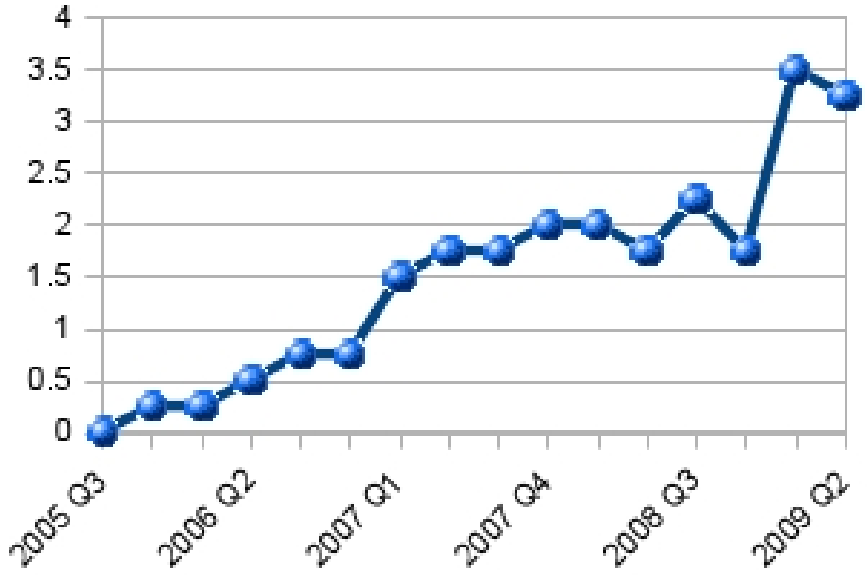
VU#476345

NVD

- National Vulnerability Database
- I count 30
- Example flow: finder → US-CERT → CERT/CC → vendor → patch → MITRE → NIST NVD
  - SISCO OSI stack
  - OPC Servers
  - Cisco Physical Access Gateway
  - Art Manion (of CERT/CC) sees trend away from neutral party disclosure

NVD

- Q1 2009 saw 10 additions – most ever
- Q2 2009 saw no additions



Average ICS vulnerabilities added to NVD per quarter using 4 quarter moving average

OSVDB

ISRCS 2009

osvdb | Search OSVDB | Browse | Vendors | Project Info | Help OSVDB! | Sponsors | hosting provided by LAYERED TECHNOLOGIES

DONATE NOW!

User Status

Account

Quick Searches

General Search Go

Title Search Go

OSVDB ID Lookup Go

Vendor Search Go

Advertisements

Ads by Google

ClearSCADA
PC-Based SCADA Host Software developed by Control Microsystems
www.clearscada.com

SCADA Controls/Telemetry

Alter Search | Results: 20 : Show Descriptions | Sort by: Score Disclosure OSVDB_ID

Search Query: vuln_title: scada text_type: alltext

ID	Disc Date	CVE	Title
54272	2009-02-09	2009-0216	GE Fanuc Proficy HMI/SCADA iFIX Obfuscated Authentication Credential Weakness
54273	2009-02-09	2009-0216	GE Fanuc Proficy HMI/SCADA iFIX Crafted Software Module Authentication Bypass
54274	2009-02-09	2009-0216	GE Fanuc Proficy HMI/SCADA iFIX External Media Autorun Environment Protection Bypass
54266	2009-02-05	2009-0210	AREVA e-terrahabitat MLF Application Unspecified Remote Overflow
54267	2009-02-05	2009-0211	AREVA e-terrahabitat WebFGServer Application Unspecified Remote DoS (PD32018)
54268	2009-02-05	2009-0212	AREVA e-terrahabitat WebFGServer Application Unspecified Remote DoS (PD32020)
54269	2009-02-05	2009-0213	AREVA e-terrahabitat NETIO Application Unspecified Remote DoS
54270	2009-02-05	2009-0214	AREVA e-terrahabitat WebFGServer Application Unspecified Remote Privilege Escalation
51546	2008-11-29	2008-5848	Advantech ADAM-6000 Module Default Password
48606	2008-09-26	2008-4322	DATAC RealWin Crafted INFOTAG / SET_CONTROL Packet Handling Remote Overflow
48533	2008-09-25	2008-2474	ABB PCU400 X87 Multiple IEC Protocol Handling Remote Overflow
46105	2008-06-11	2008-2639	CitectSCADA ODBC Service Remote Overflow
44801	2008-05-05	2008-2005	Wonderware SuiteLink Service (slssvc.exe) Crafted Registration Packet Remote DoS
40745	2008-01-25	2008-0176	CIMPLICITY w32rtr.exe Crafted IP Packet Overflow
51002	2008-01-15		Phoenix Contact FL IL 24 BK-PAC Vulnerability Scan Remote DoS
51003	2008-01-15		Lantronix MSS485-T Vulnerability Scan Remote DoS

OSVDB

- Open Source Vulnerability Database (OSVDB)
- I count NVD (30) + 3
- Researcher → mail list (e.g. FD, bugtraq) → community notices → submits to OSVDB
- Examples: Phoenix contact, Lantronix

Re: [Full-disclosure] scada/plc gear

gmaggro
Tue, 15 Jan 2008 10:12:59 -0800

The Phoenix Contact 'FL IL 24 BK-PAC' arrived the other day. It is a wonderfully German piece of DIN rail (http://www3.telus.net/public/dt0116/items/dinrails.jpg) gear:

http://eshop.phoenixcontact.com/phoenix/images/productimages/large/20260_1000_int_04.jpg
http://eshop.phoenixcontact.com/phoenix/treeViewClick.do?UID=2862314

There is a two digit LED display on it, with a reset button underneath. As soon as I saw that, I figured stability would be an issue. This turned out to be a correct assumption. While the most agressive of nmap scans did not lock it up for me, Nessus (with everything enabled) did every time. Normally the display reads '82' but when it goes south it reads '88'.

Security vendors and practitioners

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

C4
Command·Control·Conquer·Cure

WST

ZERO DAY
INITIATIVE

ALIENVAULT
CREATORS OF OSSIM

iDefense Labs
Security & Vulnerability Research Labs

INL Idaho National Laboratory
Operated by Battelle Energy Alliance

Security vendors and practitioners

ISRCS 2009

- Security vendors and practitioners
- 1017
- Discovery (e.g. reverse engineering, fuzzing)
- Purchase (Tipping Point ZDI, iDefense VCP)
- Examples
  - Wurldtech (Delphi 1000+, 16 per device)
  - AlienVault
  - Other posts from researchers
  - May not end up in DB

Intentional leakage?

<cipp at news.infracritical.com>List,

I'm currently consulting for a utility company who installed a third party device that replicates internal network data on the WAN interface regardless of configuration. After initial investigations it appears the it is a firmware bug that connot be corrected via device configuration. The Internal network is an electrical SCADA network. In brief the SCADA network broadcast traffic is being sent to the devices default gateway and would be visible upstream of the SCADA network on the public internet.

The device in question is being sold using the tag line "Industrially Hardened And Commercial Grade Security Appliance", and further more lists as a feature, "NERC CIP-compliant security". The manufacturer of the device has been contacted but has showed little interest in fixing the problem. What avenues could be explored to compel unnamed manufacturer to fix the device or remove the "NERC CIP-compliant security" claim from sales literature? What are the legal ramifications?

Google "industrially hardened and commercial grade Search Advanced Search Preferences

Web Show options... Results 1 - 4 of 4 for "industrially harden

Secure SCADA & Serial Legacy Protocol to IP, via WAN, wireless ...
Industrially Hardened And Commercial Grade Security Appliance. BANDIT II™, the latest addition to the Encore's BANDIT™ (Broadband Access Network Device for ...
www.teleprime.com/web/Products/Data/DataProducts.htm - Cached - Similar

BANDIT II™ - Industrially Hardened Security Appliance
Industrially Hardened And Commercial Grade Security Appliance. BANDIT II™, the latest addition to the Encore's BANDIT™ (Broadband Access Network Device for ...
www.encorenetworks.com/click_ds_BANDIT_2.htm - Cached - Similar

ICS Vendors

ISRCS 2009

Rockwell Automation

Honeywell

ABB Power and productivity for a better world™

SIEMENS

invensys. Wonderware

EMERSON Process Management

GE Fanuc Intelligent Platforms

OSI opening your world

TELVENT

LiveData Leading the way in real-time integration and display

AREVA

ICS Vendors

ISRCS 2009

- Product support announcements
- Lots of these, I can point to 5
- Description of how a vulnerability ends up in vendor hands
  - internal testing
  - external information (e.g. Microsoft patches)
- Example: ICONICS

ICONICS

ISRCS 2009

❖ Jan 2007

Home | FAQ | Contact | Privacy Policy

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Vulnerability Notes Database

Search Vulnerability Notes

Vulnerability Notes Help Information

View Notes By

Name

ID Number

Vulnerability Note VU#251969

ICONICS Dialog Wrapper Module ActiveX control vulnerable to buffer overflow

Overview

ICONICS Dialog Wrapper Module ActiveX control contains a buffer overflow. This vulnerability may allow a remote attacker to execute arbitrary code on a vulnerable system.

I. Description

OLE for Process Control (OPC) is a specification for a standard set of OLE COM objects for use in the process control and manufacturing fields. ICONICS provides OPC-based visualization software.

ICONICS

ISRCS 2009

- Found by CERT/CC using software now open source in demo OPC ActiveX controls
- Sep 2008: researcher posts exploit to Milw0rm
- Oct 2008: Blog reports Web-hosted exploit
- Oct 2008: US-CERT issues CIIN-08-302-01
  - Criticism repeated
- Look deeper: vuln in DlgWrapper.dll
- Jan 2007 common component update includes new DlgWrapper.dll

ICONICS

==========

Files Included in this zipped archive:

1. DlgWrapper.dll (version 9.0.166.0) *
2. HF-CommomComponent_Dec2006.txt

* This hot fix is compatible with all versions up to v9.01.

==========

Disclaimer :

IT IS UNDERSTOOD THAT THE PRODUCT SERVICE RELEASE ALTHOUGH EXTENSIVELY TESTED, MAY CONTAIN DEFECTS AND ICONICS MAKES NO EXPRESS OR IMPLIED WARRANTY OF ANY KIND. ICONICS SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES THE PRODUCT MAY HAVE REGARDING MERCHANT ABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE USER SHALL HAVE THE SOLE RESPONSIBILITY FOR ADEQUATE PROTECTION AND BACK-UP OF THE DATA USED IN CONNECTION WITH THE TESTING AND USE OF THE PRODUCT.

The User agrees that ICONICS shall not be responsible for any loss or damage to the User, its customers, clients, employees, or any third parties caused by either failure of the Product or oversight in the technical support services rendered by ICONICS.

The User agrees to indemnify and hold ICONICS harmless from any liability, loss, cost, damage, or expense, including attorney's fees, as a result of any claims which may be made by any person, third parties, that arise out of or result from the manufacture, delivery, actual, or alleged ownership, performance, use, operation, possession of the Product.

(close window)

CERTIFIED FOR

CERTIFIED FOR

Microsoft GOLD CERTIFIED

2008 ISV/SOFTWARE SOLUTIONS
PARTNER OF THE YEAR-WINNER

Issues in public disclosure

ISRCS 2009

- OEM/third party make it difficult to track down what is vulnerable
- Examples
  - Microsoft announcements and vendor testing (Direct X early July 2009)
  - Rockwell Automation Ethernet Bridge Web server (Feb 2009)
  - ABB's Markus Braendle: vendors in a hard spot
  - LiveData and NukePHP
  - Art Manion CERT/CC says tracking possible

Issues in public disclosure

ISRCS 2009

- Protection
- Examples
  - AREVA - signature
  - Snort signatures by Digital Bond
  - OMRON Fins proprietary by Sourcefire
- Threat of reverse engineering
- Signature obfuscation?

Conclusion

ISRCS 2009

- There are lots of ICS vulnerabilities
- Value in looking deeper
- Solutions
  - Vendor policy:
    - Follow existing recommended practice for vuln handling
    - Security DLC
    - Greater transparency
  - Asset owners
    - Push back on vendors – demand to know
    - Share information
    - Learn to act on vulnerability information

Contact Information

Sean McBride

Critical Intelligence

Sean.McBride@critical-intelligence.com

www.critical-intelligence.com