Tutorial

Session 2c: Known ICS Vulnerabilities

Sean McBride, MA
Critical Intelligence

August 11, 2009
Idaho Falls, Idaho
Outline

- What ICS vulnerabilities do we know about?
  - NVD
  - OSVDB
  - Security vendors
  - ICS vendors

- Issues in public disclosure of vulnerability info
  - Code re-use
  - Protection
**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**
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

#### Quick Searches

- General Search
- Title Search
- OSVDB ID Lookup
- Vendor Search

#### Advertisements

- Ads by Google
- ClearSCADA
  - PC-Based SCADA Host Software developed by Control Microsystems
  - www.clearscada.com
- SCADA Controls/Telemetry

#### Results: 20

<table>
<thead>
<tr>
<th>ID</th>
<th>Disc Date</th>
<th>CVE</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>54272</td>
<td>2009-02-09</td>
<td>2009-0216</td>
<td>GE Fanuc Proficy HMI/SCADA iFIX Obfuscated Authentication Credential Weakness</td>
</tr>
<tr>
<td>54273</td>
<td>2009-02-09</td>
<td>2009-0216</td>
<td>GE Fanuc Proficy HMI/SCADA iFIX Crafted Software Module Authentication Bypass</td>
</tr>
<tr>
<td>54274</td>
<td>2009-02-09</td>
<td>2009-0216</td>
<td>GE Fanuc Proficy HMI/SCADA iFIX External Media Autorun Environment Protection Bypass</td>
</tr>
<tr>
<td>54266</td>
<td>2009-02-05</td>
<td>2009-0210</td>
<td>AREVA e-terrahabitat MLF Application Unspecified Remote Overflow</td>
</tr>
<tr>
<td>54267</td>
<td>2009-02-05</td>
<td>2009-0211</td>
<td>AREVA e-terrahabitat WebFGServer Application Unspecified Remote DoS (PD32018)</td>
</tr>
<tr>
<td>54268</td>
<td>2009-02-05</td>
<td>2009-0212</td>
<td>AREVA e-terrahabitat WebFGServer Application Unspecified Remote DoS (PD32020)</td>
</tr>
<tr>
<td>54269</td>
<td>2009-02-05</td>
<td>2009-0213</td>
<td>AREVA e-terrahabitat NETIO Application Unspecified Remote DoS</td>
</tr>
<tr>
<td>54270</td>
<td>2009-02-05</td>
<td>2009-0214</td>
<td>AREVA e-terrahabitat WebFGServer Application Unspecified Remote Privilege Escalation</td>
</tr>
<tr>
<td>51546</td>
<td>2008-11-29</td>
<td>2008-5846</td>
<td>Advantech ADAM-6000 Module Default Password</td>
</tr>
<tr>
<td>48806</td>
<td>2008-09-26</td>
<td>2008-4322</td>
<td>DATAC RealWin Crafted INFOTAG / SET CONTROL Packet Handling Remote Overflow</td>
</tr>
<tr>
<td>48533</td>
<td>2008-09-25</td>
<td>2008-2474</td>
<td>ABB PCU400 X87 Multiple IEC Protocol Handling Remote Overflow</td>
</tr>
<tr>
<td>46105</td>
<td>2008-06-11</td>
<td>2008-2639</td>
<td>CitectSCADA ODBC Service Remote Overflow</td>
</tr>
<tr>
<td>40745</td>
<td>2008-01-25</td>
<td>2008-0176</td>
<td>CIMPlexITY w32trr.exe Crafted IP Packet Overflow</td>
</tr>
<tr>
<td>51002</td>
<td>2008-01-15</td>
<td>2008-0176</td>
<td>Phoenix Contact FL IL 24 BK-PAC Vulnerability Scan Remote DoS</td>
</tr>
</tbody>
</table>
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
Security vendors and practitioners
Security vendors and practitioners

- 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?

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 cannot be corrected via device configuration. The internal network is a 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?
ICS Vendors
ICS Vendors

- 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
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.
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

  – Criticism repeated

Look deeper: vuln in DlgWrapper.dll

Jan 2007 common component update includes new DlgWrapper.dll
Files Included in this zipped archive:

1. DlgWrapper.dll (version 9.0.166.0) *
2. HF-CommonComponent_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.
Issues in public disclosure

- 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

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

- 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