IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

invensys™
Operations Management

Security Research and Responsible Disclosure

David Baker – IOActive

Marty Edwards – DHS/INL

Ernest A. Rakaczky - Invensys

October 27, 2010

IOActive Background

- Founded in 1998
- Up market international security services organization
- London and Seattle Headquarters,
- Presence in 8 countries
- Specializing in
  - Software Assurance
  - Security Development Lifecycle
  - Infrastructure Audit
  - Industrial Control Systems Security Assessments
  - Embedded Device Security Assessments

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

invensys™
Operations Management

Highlights

- Briefed congress on Software Security in 2009
- Leadership in the computer research community
  - Smart meters / ATM / DNS / HID
- Frequent speakers at conferences such as RSA, InfoSecurity, BlackHat, Ruxcon, Defcon, Shakacon and CanSec
- Founding members of the Cloud Security Alliance

Security Research

- Independent research is key to security advances
- Boutique firms and government labs are leading the research
- ICS and embedded devices are a particularly fertile ground for research
- The security research feedback loop appears to work well in many industry segments, but is sorely remiss in others

Responsible Disclosure

- Critical security flaws require diligent and careful communication to the vendors and corresponding industry
- After remediation and patching – disclosure to the community at large needs to occur
- Community discussion encourages expertise, new ideas, and ultimately better security solutions
- The rapid security advances in AMI devices in the last two years is a great example of how well disclosure works

Responsible Disclosure

Review of:

Vulnerability Note VU#703189
Invensys Wonderware Archestra ConfigurationAccessComponent ActiveX control stack buffer overflow

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

invensys™
Operations Management

Responsible Disclosure

The value of Collaboration….

Three key partners

- The Professional Research Company
- The Responsive Vendor
- The ICS-CERT/CERT-CC

"Underlying ability to Trust"

Responsible Disclosure

The value of Collaboration….

From Day-1 - March 23rd IOActive and Invensys establish overall requirements from each other…

- Vendor Validation
- Vendor Progression
- Joint participation in Public Launch
- Mitigation requirements/patches time-line set – 90 days

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

invensys™
Operations Management

Responsible Disclosure

The value of Collaboration….

From Day-1 Ability to make organizational contact

- LinkedIn contact made on the 23rd @ 9:17PM
- Had established creditability and confidence that voice contact established 11:00AM on the 24th
- The Invensys Cyber Security Team where already in the process of validating and replicating the findings from IOActive
- Arrange Face-to-Face meeting on April 8th

Responsible Disclosure

The value of Collaboration….

From Day-1 - March 23rd to July 1 IOActive and Invensys establish frequent communications and progress status updates

- Better part of April and May spent on preparing required code patches
- June completed full testing of all required Patches – Several patch versions
- July finalized Customer Notifications and guidance

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

invensys™
Operations Management

Responsible Disclosure

The value of Collaboration… Final Stages of Disclosure…

- Early July Contacted both CERT-CC and ICS-CERT… established trust within both Cert's and prior dealings both from IOActive and Invensys
- ICS-CERT reviewed and promoted the value of a pre-push to established Invensys Customer list… 7-10 days prior to CERT announcements
- ICS-CERT review and validated Mitigation Patches
- Mid-July officially announced on CERT Vulnerability disclosure…

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

invensys™
Operations Management

Responsible Disclosure

Special Thanks –

First to IOActive, for their true value that only a research company can bring to the table, from the actual work of discovery, to ensuring Invensys had a complete understanding and their constant patience as Invensys prepared the mitigation requirements.

Second to both ICS-CERT and CERT CC for not only providing the guidance and validation but the confidence we acted in the most professional manner…

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

invensys™
Operations Management

Responsible Disclosure

From Discovery to Mitigation Launch….104 days….

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

invensys™
Operations Management