ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

# ICS-CERT ADVISORY

## ICSA-12-177-02—INVENSYS WONDERWARE INTOUCH 10 DLL HIJACK

July 23, 2012

## OVERVIEW

ICS-CERT originally released Advisory ICSA-12-177-01P on the US-CERT Portal on July 05, 2012. This web page release was delayed to provide the vendor time to contact customers concerning this information.

Independent researcher Carlos Mario Penagos Hollmann has identified an uncontrolled search path element vulnerability, commonly referred to as a dll hijack, in Invensys's Wonderware InTouch application. Successfully exploiting this vulnerability could lead to arbitrary code execution.

ICS-CERT has coordinated the report with Invensys, which has produced an upgrade to address this vulnerability. Mr. Hollmann has validated that the upgrade resolves the reported vulnerability.

## AFFECTED PRODUCTS

A vulnerability has been discovered in a common dll component used by InTouch and other Wonderware System Platform products. The following Invensys products contain the vulnerable dll and are affected:

- InTouch 2012 and all prior versions,
- Wonderware Application Server 2012 and prior versions,
- Wonderware Information Server 4.5 and prior versions,
- Foxboro Control Software 4.0 and all prior versions,
- InFusion CE/FE/SCADA 2.5 and all prior versions,
- InBatch 9.5 SP1 and all prior versions, and
- Wonderware Historian 10.0 SP1 and all prior versions.

## IMPACT

Successful exploitation of this vulnerability may lead to arbitrary code execution.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

## BACKGROUND

The Invensys Wonderware InTouch HMI is used in many industries worldwide, including manufacturing, energy, food and beverage, chemical, and water and wastewater.

The Information Server provides industrial information content including process graphics, trends, and reports. The Invensys Wonderware InTouch HMI Web Client provides access to these reports, analyses, and write back capabilities to processes.

# VULNERABILITY CHARACTERIZATION

## VULNERABILITY OVERVIEW

### UNCONTROLLED SEARCH PATH ELEMENT[a]

InTouch uses an open or uncontrolled search path to find resources, which could allow an unauthorized user to easily locate and exploit one or more locations. An unauthorized user could place a malicious dll in a directory where it could be loaded before the valid dll. An attacker must have access to the host file system to exploit this vulnerability. The exploit is only triggered when a local user runs the vulnerable application and loads a malformed dll file.

CVE-2012-3005[b] has been assigned to this vulnerability. A CVSS v2 Base Score of 6.6 has also been assigned; the CVSS vector string is (AV:L/AC:M/Au:S/C:C/I:C/A:C).[c]

[a] CWE-427 Uncontrolled Search Path Element, http://cwe.mitre.org/data/definitions/427.html, Web site last visited July 23, 2012.

[b] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3005, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[c] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:L/AC:M/Au:S/C:C/I:C/A:C), Web site last visited July 23, 2012.

## VULNERABILITY DETAILS

### EXPLOITABILITY

This vulnerability cannot be exploited remotely or without user interaction. The exploit is only triggered when a local user runs the vulnerable application and loads a malformed dll file.

### EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

### DIFFICULTY

An attacker with a moderate skill level would be able to exploit this vulnerability.

## MITIGATION

Invensys has provided instructions and a link to the software download that can be found here:

https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx

Any machine running one or more of the products listed above is affected and should be patched. No other components of the Wonderware installed products are affected. Install the Security Update using instructions provided in the ReadMe file for the product and component being installed. In general, the user should:

- Read the installation instructions provided with the patch,
- Shut down any of the affected software products,
- Install the update, and
- Restart the software.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[d] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

- Do not click Web links or open unsolicited attachments in email messages
- Refer to Recognizing and Avoiding Email Scams[e] for more information on avoiding email scams
- Refer to Avoiding Social Engineering and Phishing Attacks[f] for more information on social engineering attacks.

## ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

## DOCUMENT FAQ

**What is an ICS-CERT Advisory?** An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

[d] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed July 23, 2012.

[e] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed July 23, 2012.

[f] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed July 23, 2012.

**When is vulnerability attribution provided to researchers?** Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.