# ICS-CERT ADVISORY

## ICSA-11-195-01—INVENSYS WONDERWARE INFORMATION SERVER

July 26, 2011

## OVERVIEW

ICS-CERT Advisory ICSA-11-195-01P was originally released to the US-CERT Portal on July 14, 2011. This web page release was delayed to allow users sufficient time to download and install the update.

Independent security researchers Billy Rios and Terry McCorkle have identified a stack-based buffer overflow vulnerability that exists in two different ActiveX controls used by the Wonderware Information Server product. Successful exploitation of this vulnerability could allow remote code execution on a client running vulnerable versions of the software.

ICS-CERT has coordinated with the researchers and Invensys. Invensys has issued a patch to address this vulnerability. The researchers have confirmed this patch fully resolves this reported vulnerability in both vulnerable ActiveX controls.

## AFFECTED PRODUCTS

The following Wonderware Information Server client versions are affected:

- Wonderware Information Server 3.1
- Wonderware Information Server 4.0
- Wonderware Information Server 4.0 SP1.

## IMPACT

If successfully exploited, this vulnerability could allow an attacker to execute arbitrary code on vulnerable clients at the same privilege level as the exploited process.

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

Wonderware is a brand offering of the Operations Management Division of Invensys. Invensys Operations Management is a provider of automation and information technologies and systems.

The Wonderware Information Server is used in several industries including oil and gas, chemical, power, pharmaceutical, and water and wastewater treatment.

## VULNERABILITY CHARACTERIZATION

### VULNERABILITY OVERVIEW

The Wonderware Information Server contains a stack-based buffer overflow[a] vulnerability. An attacker would need to create a specially crafted webpage or file for the client to open. Successfully exploiting the vulnerability could allow remote code execution in an affected client.

According to Invensys, the overall Common Vulnerability Scoring System (CVSS)[b] severity score for this vulnerability is 6.0 (high) but may require social engineering to exploit.

### VULNERABILITY DETAILS

#### EXPLOITABILITY

This vulnerability is remotely exploitable. User interaction is likely required to exploit this vulnerability as users must open a malicious file or website on a client with the vulnerable ActiveX control installed in order to allow the execution of code to occur.

#### EXISTENCE OF EXPLOIT

No known exploits are specifically targeting this vulnerability.

#### DIFFICULTY

A moderate set of skills are required to create a working exploit for this vulnerability. In addition, user interaction is required to successfully execute the exploit.

## MITIGATION

Invensys has developed a patch that fully resolves this vulnerability. This patch has been confirmed by the researchers. Customers of Invensys running vulnerable versions of Information Server can update their systems to the most recent patch release by following the steps provided by Invensys. In addition to applying this patch, Invensys has made additional recommendations to customers running vulnerable versions of the Information Server product.

a. http://cwe.mitre.org/data/definitions/121.html, website accessed July 14, 2011.

b. http://nvd.nist.gov/cvss.cfm?name=&vector=(AV:N/AC:H/Au:N/C:N/I:N/A:C/E:P/RL:O/RC:C)&version=2, website accessed July 14, 2011.

- Log onto Cyber Security Updates site where Invensys provides information and useful links related to their security updates: https://wdn.wonderware.com/sites/WDN/Pages/Security Central/default.aspx
- Set the security level settings in the Internet browser to Medium–High to minimize the risk of an exploit of the vulnerability.
- For information regarding how to secure industrial control systems operating in a Microsoft Windows environment, please reference the Invensys Securing Industrial Control Systems Guide

ICS-CERT also encourages asset owners to take the following defensive precautions:

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

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. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the CSSP web page. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.[c]

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

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams*[d] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[e] for more information on social engineering attacks.

c. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html.

d. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website accessed July 14, 2011.

e. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed July 14, 2011.

## ICS-CERT CONTACT

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

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

## 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.