ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

CONTROL SYSTEMS SECURITY PROGRAM

# ICS-CERT ADVISORY

## ICSA-12-039-01—INVENSYS WONDERWARE HMI REPORTS XSS AND WRITE ACCESS VIOLATION VULNERABILITIES

February 08, 2012

## OVERVIEW

Independent security researchers Billy Rios and Terry McCorkle have identified cross-site scripting (XSS) and write access violation vulnerabilities in the Invensys Wonderware HMI reports product.

ICS-CERT has coordinated these two vulnerabilities with Invensys, which has produced a new product version that resolves these reported vulnerabilities. The researchers have confirmed that the new version resolves these vulnerabilities.

## AFFECTED PRODUCTS

According to Invensys, the following versions are affected:

- Wonderware HMI Reports 3.42.835.0304 and prior.

## IMPACT

Successful attacks could result in data leakage, denial of service, or remote 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 these vulnerabilities based on their 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.

According to Invensys, Wonderware HMI Reports is deployed across several industries including manufacturing, building automation, oil and gas, water and wastewater, healthcare, and electric utilities. Invensys states that these products are used worldwide.

# VULNERABILITY CHARACTERIZATION

## VULNERABILITY OVERVIEW

### CROSS-SITE SCRIPTING

A XSS[a] vulnerability exists in the Invensys Wonderware HMI Reports application because of a lack of server-side validation of query string parameter values. Exploitation of this vulnerability requires that a user visit a specially crafted URL, which injects client-side scripts into the server's HTTP response to the client.

CVE-2011-4038[b] has been assigned to this vulnerability, which is identical to ICS-CERT Advisory "ICSA-12-024-01 – Ocean Data Systems Dream Reports XSS and Write Access Violation Vulnerabilities." Invensys' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 6.0.

### WRITE ACCESS VIOLATION

A write access violation[c] vulnerability exists in the Invensys Wonderware HMI Reports application. Exploitation of this vulnerability requires that a user opens a specially crafted file. This may result in arbitrary code execution.

CVE-2011-4039[d] has been assigned to this vulnerability, which is identical to ICS-CERT Advisory "ICSA-12-024-01 – Ocean Data Systems Dream Reports XSS and Write Access Violation Vulnerabilities." Invensys' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 6.0.

## VULNERABILITY DETAILS

### EXPLOITABILITY

The XSS vulnerability is remotely exploitable.

The write access violation is not remotely exploitable and cannot be exploited without user interaction. The exploit is only triggered when a local user runs the vulnerable application and loads a malformed file.

### EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

[a] http://cwe.mitre.org/data/definitions/80.html

[b] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4038, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[c] http://cwe.mitre.org/data/definitions/119.html

[d] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4039, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

## DIFFICULTY

An attacker with a low skill level can create the XSS exploit. Social engineering is required to convince the user to visit a malicious site.

Crafting a working exploit for the access violation vulnerability would be difficult. Social engineering is required to convince the user to accept the malformed file. Additional user interaction is needed to load the malformed file. This decreases the likelihood of a successful exploit.

## MITIGATION

Invensys recommends users install the Security Update using specific instructions provided in each ReadMe file for each product and component being installed. In general, users should download the update, the associated upgrade instructions, and the license file update. After installation, users must migrate the report definitions into the new Quick Reports 2012 format, as explained in the upgrade instructions. Users must also request a permanent license file from the distributor.

Customers can access the update at the following website:

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

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.*[e] 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:

1. Do not click web links or open unsolicited attachments in e-mail messages

[e] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed February 08, 2012.

2. Refer to *Recognizing and Avoiding Email Scams*[f] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[g] for more information on social engineering attacks.

## 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.

***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.

[f] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed February 08, 2012.

[g] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed February 08, 2012.