ICS-CERT ADVISORY

ICSA-12-062-01—INVENSYS WONDERWARE INFORMATION SERVER MULTIPLE VULNERABILITIES

April 02, 2012

OVERVIEW

ICS-CERT originally released Advisory "ICSA-12-062-01P—Invensys Wonderware Information Server Multiple Vulnerabilities" on the US-CERT secure portal on March 02, 2012. This web page release was delayed to allow users time to download and install the update.

Independent security researchers Terry McCorkle and Billy Rios have identified multiple vulnerabilities in the Invensys Wonderware Information Server. Invensys has developed a security update to address these affected products.

Invensys has expressed appreciation to Billy Rios and Terry McCorkle as independent security researchers for the discovery and collaboration with Invensys on resolving these vulnerabilities.

AFFECTED PRODUCTS

The following Invensys Wonderware Information Server versions are affected:

- 4.0 SP1 and 4.5—Portal
- 4.0 SP1 and 4.5—Client.

The following Invensys Wonderware Historian Client version is affected:

Only Wonderware Historian Client versions installed on the same node as the Wonderware Information Server Portal or Client are subject to the vulnerabilities reported in this Advisory.

IMPACT

These vulnerabilities, if exploited, could allow denial of service, information disclosure, remote code execution, or session credential high jacking. 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 operational environment, architecture, and product implementation.

.

BACKGROUND

The Invensys[a] Wonderware Information Server 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 Information Server Web Clients provides access to reports, analysis, or write back capabilities to processes.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

CROSS-SITE SCRIPTING[b]

This vulnerability enables an attacker to inject client side script into web pages viewed by other users or bypass client side security mechanisms imposed by modern web browsers. This vulnerability, if exploited, could allow arbitrary code execution and may require social engineering to exploit.

CVE-2012-0225[c] has been assigned to this vulnerability. The Invensys assessment of the compound vulnerabilities using the CVSS[d] Version 2.0 calculator rates an Overall CVSS Score of 8.1.[e]

SQL INJECTION[f]

This vulnerability can be used by an attacker to perform database operations that were unintended by the web application designer and, in some instances, can lead to total compromise of the database server. This vulnerability, if exploited, could allow arbitrary code execution.

CVE-2012-0226[g] has been assigned to this vulnerability. The Invensys assessment of the compound vulnerabilities using the CVSS[h] Version 2.0 calculator rates an Overall CVSS Score of 8.1.[e]

PERMISSIONS, PRIVILEGES, AND ACCESS CONTROLS[i]

The security access permissions issues with client controls can lead to denial of service.

CVE-2012-0228[j] has been assigned to this vulnerability. The Invensys assessment of the compound vulnerabilities using the CVSS[k] Version 2.0 calculator rates an Overall CVSS Score of 8.1.[e]

---

a. http://www.invensys.com/, website last accessed March 29, 2012.

b. http://cwe.mitre.org/data/definitions/79.html, website last accessed March 29, 2012.

c. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0225, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

d. http://nvd.nist.gov/cvss.cfm, website last accessed March 29, 2012.

e. National Vulnerability Database Calculator for LFSEC00000069 ,website last accessed March 29, 2012.

f. http://cwe.mitre.org/data/definitions/89.html, website last accessed March29, 2012.

g. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0226, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

h. http://nvd.nist.gov/cvss.cfm, website last accessed March 29, 2012.

i. http://cwe.mitre.org/data/definitions/264.html, website last accessed March 29, 2012.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level can create the denial of service, whereas it would require a more skilled attacker to execute arbitrary code. This attack may require social engineering to exploit.

MITIGATION

Invensys has developed software updates to address the reported vulnerabilities. Customers of Invensys running vulnerable versions of Invensys Wonderware Information Server and Invensys Wonderware Historian Client can update their systems to the most recent software updates released by following the steps provided by Invensys.

Invensys software updates can be downloaded from the Wonderware Development Network ("Software Download" area) and the Infusion Technical Support website: https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx.

The following steps are provided by Invensys for update information.

Install the Security Update using instructions provided in the ReadMe file for the product and component being installed. In general, the user should proceed as indicated below:

1. Wonderware Information Server – Portal component: Run the "Hotfix Install Utility."
2. Wonderware Information Server – Client component: Uninstall the client from Add/Remove Programs (ClientSetup.msi), clear the IE cache (see specific instructions in the Readme file provided with the Security Update) and access the Wonderware Information Server site.
3. If Step 2 and Step 3 are on the same node, perform the functions in Step 2 and also run the "Hotfix Install Utility."

In addition to applying the software updates, Invensys has made additional recommendations to customers running vulnerable versions of the Invensys Wonderware Information Server and Invensys Wonderware Historian Client products. Customers using versions of the products prior to Invensys Wonderware Information Server 5.0 and Invensys Wonderware Historian Client 10 SP3 should apply the security update to all nodes where the Portal and Client components are installed. (All browser clients of the portal are affected and should be patched). Customers using the affected versions of Invensys

---

j. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0228, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

k. http://nvd.nist.gov/cvss.cfm, website last accessed March 29, 2012.

Wonderware Information Server should set the security level settings in the Internet browser to "Medium – High" to minimize the risks presented by these vulnerabilities.

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*.[l] 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
2. Refer to *Recognizing and Avoiding Email Scams*[m] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[n] 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

l. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed March 29, 2012.

m. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed March 29, 2012.

n. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed March 29, 2012.

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.