ICS-CERT ADVISORY

ICSA-11-332-01—INVENSYS WONDERWARE INBATCH ACTIVEX VULNERABILITIES

December 20, 2011

OVERVIEW

ICS-CERT originally released advisory "ICSA-11-332-01P —Invensys Wonderware InBatch ActiveX Vulnerabilities" in the US-CERT secure portal on November 28, 2011. This web page release was delayed to allow users time to download and install the update.

Researcher Kuang-Chun Hung of the Security Research and Service Institute–Information and Communication Security Technology Center (ICST) has identified three vulnerabilities in Invensys Wonderware InBatch. These vulnerabilities exist in the GUIControls, BatchObjSrv, and BatchSecCtrl ActiveX controls.

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code or cause a denial of service (DoS) on systems with affected versions of Wonderware InBatch Runtime Client components.

ICS-CERT has coordinated the report with the ICST and Invensys. Invensys has issued software updates that resolve these vulnerabilities. The ICST has confirmed the software updates fully resolve the reported vulnerabilities.

AFFECTED PRODUCTS

The following Invensys Wonderware InBatch versions are affected:

- 8.1 SP1, 9.0 SP2, and 9.5—InBatch Server and Runtime Clients
- 9.0 and 9.0 SP1.

The affected components exist in a variety of Wonderware products including InTouch and Information Server browser clients that have downloaded converted windows that contain these controls.

According to Invensys, I/A Series Batch 8.1 SP1 and Wonderware InBatch 9.5 SP1 and higher are not affected by these vulnerabilities.

IMPACT

If successfully exploited, these vulnerabilities could allow an attacker to execute arbitrary code on systems running affected versions of the product.

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

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

The InBatch Runtime Client provides an interface to the batch management system to allow operator interaction during the batch execution.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

Affected versions of the InBatch Runtime Client components contain three buffer overflow[a,b] vulnerabilities. These vulnerabilities could be exploited by using long string values for the properties/methods of the referenced controls. This could result in either a DoS or remote code execution running with privileges of the logged-in user.

CVE-2011-3141[c] has been assigned to this vulnerability. Invensys has assessed the vulnerabilities using the CVSS[d] Version 2.0 calculator and gives the Overall CVSS = 6.0. Click here to review the assessment.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable. This exploit may require social engineering.

EXISTENCE OF EXPLOIT

No publicly known exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level can create the DoS; a more skilled attacker could exploit the vulnerability to execute arbitrary code.

MITIGATION

Invensys has developed software updates to address the reported vulnerabilities. Invensys recommends that customers who are running vulnerable versions of Wonderware InBatch update their systems to either InBatch 9.0 SP2 or 9.5 on all nodes that have the InBatch client runtime and the InBatch Server installed. Installation does not require a reboot.

a. http://cwe.mitre.org/data/definitions/121.html, website accessed November 28, 2011.
b. http://cwe.mitre.org/data/definitions/122.html, website accessed November 28, 2011.
c. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3141, website last accessed November 28, 2011.
d. http://nvd.nist.gov/cvss.cfm, website last accessed November 28, 2011.

Customers can download updates from the "Software Download" section of the Invensys Customer First Support website:

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

Follow the instructions in the ReadMe section for the product and component to install the software update.

In addition to applying the software updates, Invensys has made additional recommendations to customers running vulnerable versions of the Invensys Wonderware InBatch product:

- Set the security level settings for the Internet browser to Medium−High to minimize the risk of a vulnerability exploit.
- Reference the Invensys Securing Industrial Control Systems Guide for additional information on securing industrial control systems operating in a Microsoft Windows environment.

To access information related to Invensys security updates, customers can logon to the Cyber Security Updates website and the GCS Foxboro Wonderware Security Releases webpage:

https://wdn.wonderware.com/sites/WDN/Pages/Security Central/default.aspx

http://support.ips.invensys.com/content/WDN/HTM/ww_security.asp.

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 system 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.

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed November 28, 2011.

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*[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 November 28, 2011.
g. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed November 28, 2011.