ICS-CERT ADVISORY

ICSA-11-094-01—WONDERWARE INBATCH CLIENT ACTIVEX BUFFER OVERFLOW

April 13, 2011

OVERVIEW

ICS-CERT has received a report from independent security researcher Jeremy Brown regarding a buffer overflow vulnerability in a Wonderware InBatch Client ActiveX control.

According to the researcher's report, the client ActiveX control is vulnerable to a buffer overflow that could cause denial of service (DoS) or the possible execution of arbitrary code in older versions. In order to successfully exploit this vulnerability, the attacker must direct the InBatch client user to a malicious host. This exploit requires the attacker to perform social engineering. Invensys has validated the researcher's claim and has developed a patch to mitigate this vulnerability. ICS-CERT has verified that the provided security patch resolves the vulnerability.

AFFECTED PRODUCTS

This vulnerability affects custom runtime client programs of all supported versions of the Wonderware InBatch Server products. Invensys has supplied Table 1, which identifies which currently supported products are affected.

Table 1. Invensys supported products affected by this vulnerability.

Product and Component	Supported Operating System	Security Impact	Severity Rating
Wonderware InBatch 8.1—InBatch Runtime Clients (all versions)	Windows XP Professional Windows 2000 Server Windows Server 2003	Denial of Service Remote code execution	Medium
Wonderware InBatch 9.0—InBatch Runtime Clients (all versions)	Windows XP Professional Windows Server 2003 Windows Server 2008	Denial of Service	Medium

IMPACT

While a successful exploit of the buffer overflow could allow a DoS or arbitrary code execution, the specific impact to an individual organization depends on many factors that are unique to the organization.

ICS CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and operational product implementation.

BACKGROUND

According to Invensys, Wonderware InBatch is used to develop batch management capabilities for control system applications that run on the Microsoft Windows platforms. The ActiveX control is supplied for end users to build custom runtime client interfaces to the InBatch Server.

Wonderware InBatch software is used in a wide variety of batching processes including pharmaceutical production; food and beverage production, including breweries and milk production; and various Chemical Sector batching processes. InBatch software is estimated to be deployed in Europe (60%), North America (30%), and other areas around the world (10%).

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

According to the researcher's report, the InBatch client ActiveX control will connect to an InBatch servervia TCP. If an attacker successfully employs social engeneering (i.e., phishing e-mail), the user could be connected to a malicious server. Once connected to this server, the InBatch client ActiveX is vulnerable to a buffer overflow that could allow a DoS or possibly lead to arbitrary code execution.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is not remotely exploitable.

EXISTENCE OF EXPLOIT

Currently, no known exploits are specifically targeting this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability would be difficult. Social engineering is required to convince the user to access a malicious host.

MITIGATION

ICS-CERT and Invensys recommend that users of the Wonderware InBatch runtime client ActiveX control take the following mitigation steps:

- Install the patch provided from Invensys. Registered users please log into the Wonderware Developer Network or contact Wonderware Tech Support.
- Log onto Cyber Security Updates site where Invensys provides information and useful links related to their security updates: http://iom.invensys.com/EN/Pages/CyberSecurityUpdates.aspx

Organizations that observe 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 System Security Program also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[a]

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*[b] for more information on avoiding e-mail scams.
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[c] 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 Control Systems Security Program 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.

a. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website accessed March 3, 2011.
b. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf., website accessed March 3, 2011.
c. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website accessed March 3, 2011.