



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-10-348-01—WONDERWARE INBATCH AND I/A SERIES BATCH BUFFER OVERFLOW

December 14, 2010

OVERVIEW

An independent security researcher has published information to a vulnerability disclosure website regarding a buffer overflow vulnerability in the Wonderware InBatch and I/A Series Batch software products (all supported versions).

According to the researcher's report, the service listening on TCP Port 9001 is vulnerable to a buffer overflow that could cause denial of service (DOS) or the possible execution of arbitrary code. This vulnerability is remotely exploitable and exploit code is publicly available. Invensys has validated the researcher's claim and is developing a patch to mitigate this vulnerability.

ICS-CERT is coordinating this vulnerability disclosure with Invensys and the CERT Coordination Center (CERT/CC).

AFFECTED PRODUCTS

This vulnerability affects all supported versions of the Wonderware InBatch Server and I/A Batch Server in the InBatch and I/A Batch products. The following table from Invensys identifies the currently supported products that are affected:

Product and Component	Supported Operating System	Security Impact	Severity Rating
Wonderware InBatch 8.1 - InBatch Server (all versions)	Windows XP Professional Windows 2000 Server Windows Server 2003	Denial of Service	Medium
Wonderware InBatch 9.0 - InBatch Server (all versions)	Windows XP Professional Windows Server 2003	Denial of Service	Medium
I/A Series Batch 8.1 - I/A Series Batch Server (all versions)	Windows Server 2003 Server R2 Windows XP Professional SP2	Denial of Service	Medium

Users running earlier versions should contact their support provider for guidance.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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 product implementation.

BACKGROUND

According to Invensys, Wonderware InBatch and I/A Series Batch products are used to develop batch management capabilities for control system applications that run on the Microsoft Windows platforms.

Wonderware InBatch and I/A Series Batch 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%). I/A Series Batch software is estimated to be deployed in North America (60%), and Europe (40%).

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

According to the researcher's report, the InBatch service listening on TCP Port 9001 is vulnerable to a buffer overflow that could allow a DOS or possibly lead to arbitrary code execution. This vulnerability is remotely exploitable and exploit code has been released.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

Exploit code specifically targeting this vulnerability has been released.

DIFFICULTY

It is estimated that an attacker would require an intermediate skill level to exploit this vulnerability. An exploit would require development of a malicious application with access to TCP Port 9001 on the batch server and an understanding of the protocol used on that port. The malicious application would need to send a partially valid message that overflows the internal buffer.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Invensys has internally assessed the vulnerability using the Vulnerability Scoring System (CVSS) and has determined this vulnerability rates an Overall CVSS score of 5.5, using the CVSS Version 2.0 calculator.¹

MITIGATION

ICS-CERT and Invensys recommend that users of Wonderware InBatch and I/A Series Batch take the following mitigation steps:

- Install the patch when it is released. ICS-CERT will provide an update to this Advisory when a patch is released.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.²
- Control system networks and devices should be located behind firewalls and isolated from the business network. Access to TCP Port 9001 should be restricted. If remote access is required, secure methods such as Virtual Private Networks (VPNs) should be utilized.

Invensys provides information and useful links related to their security updates at their [Cyber Security Updates](#) site.

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

The Control System Security Program also provides a recommended practices section for control systems on the United States Computer Emergency Readiness Team (US-CERT) web site. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.³

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 System Security Program Information and Incident Reporting: www.ics-cert.org

1. NIST, <http://nvd.nist.gov/cvss.cfm>, web site last visited December 14, 2010.

2. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, web site last visited December 3, 2010.

3. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html.