Invensys Operations Management Security Bulletin

Title

Stack Based buffer overflow in the “Label” method, in the InBatch BatchField ActiveX Control (CR LFSEC00000054)

Rating

Medium

Published By

Invensys Operations Management Security Response Center

Overview

A *vulnerability* has been discovered in the InBatch BatchField ActiveX Control. This vulnerability, if exploited, could cause a stack based buffer overflow. In Wonderware InBatch 9.0 and newer versions of the product this could cause the hosting application (container) to shutdown. In pre-9.0 versions it could also allow the possibility of remote execution. The rating is Medium (for InBatch 9.0 and higher versions) and High (for pre 9.0 versions) and may require social engineering to exploit. Social engineering is when people are unknowingly manipulated to perform certain actions that may be detrimental to the system. For example, asking an end-user to click on an email link to a rogue site or download a malicious file.

This security bulletin announces that software updates are available to customers running Wonderware InBatch on all supported versions. Please refer to the “Affected Products and components” section to access the updates.

Recommendations

Customers using versions of Wonderware InBatch should make sure that their Batch Server is on a secured network with limited or no access from the Internet. Customers using versions of Wonderware InBatch 9.0 and older that require internet access SHOULD set the Security level settings in the Internet browser to Medium - High to minimize the risk of an exploit of the vulnerability.

For information regarding how to secure Industrial Control Systems operating in a Microsoft Windows environment, please reference the Invensys Securing Industrial Control Systems Guide

NVD Common Vulnerability Scoring System

The U.S. Department of Homeland Security has adopted the common Vulnerability Scoring System (CVSS) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. The system is comprised of components: impact, exploitability and complexity as well as added determinants such as authentication and impact type. In summary, the components such as impact are given an individual score between 0.0 and 10.0. The average of all components is the overall score where the maximum is 10.0. Details about this scoring system can be found here: http://nvd.nist.gov/cvss.cfm

For InBatch 9.0 and higher versions, our assessment of the vulnerability using the CVSS Version 2.0 calculator rates an Overall CVSS Score of 4.2. To review the assessment, use this link:

http://nvd.nist.gov/cvss.cfm?name=&vector=(AV:N/AC:H/Au:N/C:N/I:N/A:C/E:P/RL:O/RC:C)&version=2

For versions previous to Wonderware InBatch 9.0, our assessment of the vulnerability using the CVSS Version 2.0 calculator rates an Overall CVSS Score of 7.3. To review the assessment, use this link:

http://nvd.nist.gov/cvss.cfm?name=&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C/E:P/RL:O/RC:C)&version=2

Customers have the option in the Environmental Score Metrics section of the calculator to further refine the assessment based on the organizational environment of the installed product. Adding the Environmental Score Metrics will assist the customer in determining the operational consequences of this vulnerability on their installation.[1]

[1] CVSS Guide

Affected Products and Components[2]

The following table identifies the currently supported products affected[3]. Software updates can be downloaded from the Wonderware Development Network ("Software Download" area) and the Infusion Technical Support websites using the links embedded in the table below.

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Update
Wonderware InBatch 8.1 – InBatch Client (all versions) (LFSEC00000054)	Windows XP Professional Windows 2000 Server Windows Server 2003	Denial of Service Remote execution	Medium	Wonderware InBatch 8.1 Client (all versions) Security Update LFSEC00000054
Wonderware InBatch 9.0 – InBatch Client (all versions) (LFSEC00000054)	Windows XP Professional Windows Server 2003 Windows Server 2008	Denial of Service	Medium	Wonderware InBatch 9.0 Client (all versions) Security Update LFSEC00000054

[2] Windows Vista and Windows XP are trademarks of the Microsoft group of companies.

[3] Customers running earlier versions may contact their support provider for guidance.

Not Affected Products and components

Wonderware InBatch 9.0 SP2 version and higher will not be affected by this vulnerability.

I/A Series Batch versions are NOT affected by the vulnerability as this offering does not use the ActiveX controls.

Background

Wonderware InBatch provides flexible batch management capabilities. The InBatch server component manages the execution of batches and related recipes in a structured way in coordination with controllers and User Interface.

The InBatch User Interface provides a set of ActiveX controls to allow easy interaction between operators and the batch execution system. The ActiveX controls are generally installed as part of the BatchServer and on all Batch Runtime clients, including InTouch and any third party InBatch Client programs (VB or C++)

Additionally the InBatch ActiveX controls can be used in published graphics in Wonderware Information Server.

[2] Registered trademarks and trademarks must be noted such as "Windows Vista and Windows XP are trademarks of the Microsoft group of companies."
[3] Customers running earlier versions may contact their support provider for guidance.

Vulnerability Characterization

The InBatch BatchField ActiveX Control contains a vulnerability that may allow remote code execution in an unsecure deployment4. In InBatch 9.0 and newer versions of the product this could cause the hosting application (container) to shutdown. In pre-9.0 versions it could also allow the possibility of remote execution on the stack.

The controls are vulnerable to cross-scripting attacks, meaning this vulnerability could be triggered by browsing to a malicious web site or opening a malicious email. The Internet browser settings have to be configured with a fairly low security setting for this to be possible and it is primarily an issue for the pre-9.0 controls because they cannot protect against remote code execution.

Any machine that the InBatch BatchField ActiveX Control is installed on is affected and must be patched. The possibilities include Wonderware InTouch or Wonderware Information Server browser clients who have downloaded converted windows that contain the controls.

No other components of Wonderware InBatch are affected.

Other Information

Acknowledgments

Invensys thanks the following for the discovery and collaboration with us on this vulnerability:

- Jeremy Brown as an independent Security Researcher for reporting the Stack Based buffer overflows (CR LFSEC00000054),
- Along with the continual support and collaboration from the ICS-CERT.

Support

For information on how to reach Invensys Operations Management support for your product, refer to this link: Invensys Customer First Support. If you discover errors or omissions in this bulletin, please report the finding to support.

Invensys Operations Management Cyber Security Updates

For information and useful links related to security updates, please visit the Cyber Security Updates site.

Cyber Security Standards and Best Practices

For information regarding how to secure Industrial Control Systems operating in a Microsoft Windows environment, please reference the Invensys Securing Industrial Control Systems Guide.

Invensys Operations Management Security Central

For the latest security information and events, visit Security Central.

[4] Any control system installation which does not follow the practices describe in the Invensys Secure Deployment Guide

Disclaimer

THE INFORMATION PROVIDED HEREIN IS PROVIDED “AS-IS” AND WITHOUT WARRANTY OF ANY KIND. INVENSYS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY INVENSYS, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES WILL CREATE A WARRANTY AND CUSTOMER MAY NOT RELY ON ANY SUCH INFORMATION OR ADVICE.

INVENSYS DOES NOT WARRANT THAT THE SOFTWARE WILL MEET CUSTOMER’S REQUIREMENTS, THAT THE SOFTWARE WILL OPERATE IN COMBINATIONS OTHER THAN AS SPECIFIED IN INVENSYS’ DOCUMENTATION OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

IN NO EVENT WILL INVENSYS OR ITS SUPPLIERS, DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY CUSTOMER OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF INVENSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. INVENSYS’ LIABILITY FOR DAMAGES AND EXPENSES HEREUNDER OR RELATING HERETO (WHETHER IN AN ACTION IN CONTRACT, TORT OR OTHERWISE) WILL IN NO EVENT EXCEED THE AMOUNT OF FIVE HUNDRED DOLLARS ($500 USD).

.