invensys™
Operations Management

Invensys Operations Management Security Alert

Title

Wonderware InBatch and Foxboro I/A Series Batch Server lm_tcp buffer overflow (LFSEC00000051)

Rating

Medium

Published By

Invensys Operations Management Security Response Center

Overview

A vulnerability has been discovered in InBatch Server and I/A Batch Server in all supported versions of Wonderware InBatch and Foxboro I/A Series Batch. This vulnerability, if exploited, could allow Denial of Service (DoS), the consequence of which is a crash of the InBatch Server. The rating is medium and would require a malicious application that has access to port 9001 on the batch server and understands the protocol used on that port to send a partially valid message that overflows an internal buffer.

This security bulletin announces that software updates are available to customers running Wonderware InBatch and I/A Series Batch on all supported versions. Please refer to the **Affected Products and Components** section for the location of the Security Updates. You can also contact Invensys Customer First Support for more information.

Recommendations

Customers using versions of Wonderware InBatch 8.1 SP1, Wonderware 9.0 Sp1 and I/A Series Batch 8.1 SP1 SHOULD apply the security update to all nodes where the InBatch Server component is installed. It is required to perform an Exit-and-Shutdown from the InBatch Environment Display. During the install of the security update, operator and configuration clients of the InBatch system are not operational.

For customers not applying the Security Updates it is highly recommended that their Batch Server is on a secured network inaccessible from the Internet. As an immediate security measure it is advised to configure the network firewall to protect port 9001.

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

Our assessment of the vulnerability using the CVSS Version 2.0 calculator rates an Overall CVSS Score of 4.8. To review the assessment, use this link

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

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]

Affected Products and Components[2]

The following table identifies the currently supported products affected[3].

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Update Download
Wonderware InBatch 8.1 – InBatch Server (all versions)	Windows XP Professional Windows 2000 Server Windows Server 2003	Denial of Service	Medium	https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx
Wonderware InBatch 9.0 – InBatch Server (all versions)	Windows XP Professional Windows Server 2003 Windows Server 2008	Denial of Service	Medium	https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx
I/A Series Batch 8.1 – I/A Series Batch Server (all versions)	Windows 2003 Server R2 SP2 or Windows XP Professional SP2	Denial of Service	Medium	https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx

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

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

Background

Wonderware InBatch and I/A Series Batch provide 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 server component is typically installed on a dedicated server with no access from the internet or corporate network.

---

[1] CVSS Guide
[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 Server component contains a vulnerability that may allow Denial of Service in an unsecure deployment[4]. The vulnerability would require a malicious application that has access to port 9001 on the batch server and understands the protocol used on that port to send a partially valid message that overflows an internal buffer.

Any machine where the InBatch Server or I/A Series Batch server is installed is affected.   No other components of Wonderware InBatch and I/A Series Batch are affected. Further mitigation beyond that identified in this Alert will be made available to customers running Wonderware InBatch and I/A Series Batch.

Update Information

Install the Security Update using instructions provided in the ReadMe for the product and component being installed. Before installing the security update, perform an Exit-and-Shutdown from the InBatch Environment Display. Be aware that operator and configuration clients of the InBatch system are not operational during this install.

Other Information

Acknowledgments

Invensys thanks Secunia (www.secunia.com), US-CERT, and ICS-CERT for their collaboration with us on this vulnerability.

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.

Disclaimer

---

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

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).