Invensys Operations Management Security Bulletin

Title

Security Bulletin - Wonderware Application Server (WAS) Bootstrap - Directory Traversal

LFSEC00000017

Rating

Medium

Published By

Invensys Operations Management Security Response Center

Overview

Invensys has discovered directory traversal type vulnerabilities in three components that are installed by the Wonderware Application Server Bootstrap. If exploited, these vulnerabilities could lead to information disclosure, malicious file upload, or arbitrary code execution. The rating is **Medium** 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 or download a file.

This security bulletin announces the software updates available to customers that have been tested on all supported versions of Wonderware Application Server, InFusion (FCS), and all products where the Wonderware Application Server bootstrap is installed.

Recommendations

Customers using supported versions of Wonderware Application Server earlier than 2012 R2 or InFusion (FCS) Version 4.0 SHOULD apply the security update to all nodes where the WAS boostrap is installed. Installation of the Security Update temporarily stops all processing but does not require a reboot.

National Vunerability Database (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 multiple 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 6.2. To review the assessment, use this link: National Vulnerability Database Calculator for LFSEC00000017. 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]. 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. In general, all nodes where the Wonderware Application Server boostrap is installed are affected and must be patched before any additional configuration or deployment can occur.

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Update
Wonderware Application Server 2012 SP1 and Prior versions	Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows 2008, Windows 2008 R2	6.2	High	Wonderware ArchestrA Bootstrap – Directory Transversal (LFSEC00000017)
FCS 4.0.x and Prior versions InFusion CE, FE, SCADA all versions	Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows 2008, Windows 2008 R2	6.2	High	Wonderware ArchestrA Bootstrap – Directory Transversal (LFSEC00000017)

Non-Affected Products

- Wonderware Application Server 2012 R2

Background

Wonderware is the market leader in real-time operations management software. Wonderware Application Server and InFusion (FCS) software are used for designing, building, deploying and maintaining standardized applications for manufacturing and infrastructure operations.

Vulnerability Characterization

A directory traversal is a programming input validation error that may allow an attacker to send a specially crafted message causing the system to allow access to regions of the file system other than the specified root. This gives an attacker the ability to move files into arbitrary locations or in extreme cases even execute malicious code.

Any machine where the Wonderware Application Server bootstrap is installed is affected, and must be patched.

[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.

Update Information

Install the Security Update on all nodes where the Wonderware Application Server boostrap is installed using instructions provided in the Readme for the product and component being installed. In general, the user SHOULD:

- Backup the Galaxy Database
- Ensure that no deployment of configuration activites are taking place on any local or remote IDE
- Run the Security Update Utility

If any problems occur, the security Update can be uninstalled using the instructions in the Readme.

Other Information

Acknowledgments

Invensys would like to thank ICS-CERT for their continuing support, coordination and assistance in producing this Security Update.

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 Invensys Operations Management 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 WDN Security Central Cyber Security Updates

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

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).

.