Invensys Operations Management Security Bulletin

Title

Security Bulletin System Platform Buffer Overflow LFSEC00000071

Rating

Medium

Published By

Invensys Operations Management Security Response Center

Overview

Cyber researcher Celil Unuver from SignalSec Corp has discovered two heap-based buffer overflow vulnerabilities in the WWCabFile component of the Wonderware System Platform that is used by the Wonderware Application Server, Foxboro Control Software, InFusion CE, InFusion FE, InFusion SCADA, InTouch, the ArchestrA Application Object Toolkit and the Wonderware Information Server. If exploited, these vulnerabilities could lead to arbitrary code execution. The rating is Medium due to the exploit difficulty and may require social engineering. 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, InTouch, ArchestrA Application Object Toolkit, Foxboro Control Software, InFusion, and Wonderware Information Server listed in the table below.

Recommendations

Customers using the following product versions SHOULD apply the security update to all nodes where the WWCabFile component of the System Platform is installed. Installation of the Security Update does not require a reboot. If multiple products are installed on the same node, the customer need only install the Security Update once.

- Wonderware Application Server 2012 and all prior versions
- Foxboro Control Software Version 3.1 and all prior versions
- InFusion CE/FE/SCADA 2.5 and all prior versions
- Wonderware Information Server 4.5 and all prior versions
- ArchestrA Application Object Toolkit 3.2 and all prior versions
- InTouch 10.0 to 10.5 only(earlier versions of InTouch are not affected)

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 6. To review the assessment, use this link: National Vulnerability Database Calculator for LFSEC00000071. 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 Invensys Global Customer Support websites using the links embedded in the following table.

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Update
Wonderware Application Server 2012 and prior versions	Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows 2008, Windows 2008 R2	6.0	Medium	System Platform 2012 Security Update LFSEC00000071
Wonderware Information Server 4.5 and prior versions	Windows Server 2003, Windows 2008, Windows 2008 R2	6.0	Medium	System Platform 2012 Security Update LFSEC00000071
Foxboro Control Software 3.1 and Prior versions, InFusion CE/FE/SCADA 2,5 and prior versions	Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows 2008, Windows 2008 R2	6.0	Medium	System Platform 2012 Security Update LFSEC00000071
ArchestrA Application Object Toolkit 3.2 and prior versions	Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows 2008, Windows 2008 R2	6.0	Medium	System Platform 2012 Security Update LFSEC00000071
InTouch 10.0 through InTouch 2012	Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows 2008, Windows 2008 R2	6.0	Medium	System Platform 2012 Security Update LFSEC00000071

[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.

Non-Affected Products

The Wonderware Historian is part of the System Platform but is not affected by this Security Update and does not need to be patched.

Background

Wonderware is the market leader in real-time operations management software. Wonderware System Platform along with the Foxboro Control Software is used for designing, building, deploying and maintaining standardized applications for manufacturing and infrastructure operations. The Wonderware Information Server is a component of the System Platform and is used for aggregating and presenting plant production and performance data over the web or company intranet.

Vulnerability Characterization

A buffer overflow is a programming error where data larger than the allocated memory space overwrites adjacent memory. There are two types, stack based and heap based, the latter of which is much more difficult to exploit.

Any machine where the **WWCabFile.dll** is installed is affected and must be patched. No other components of the System Platform are affected.

Update Information

Install the Security Update using instructions provided in the ReadMe for the product and component being installed. In general, the user SHOULD:

- Backup the Galaxy Database
- Backup the Wonderware Information Server Database
- 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 thanks the following for the discovery and collaboration with us on this vulnerability:

Celil Unuver of SignalSec Corp for reporting the Wonderware System Platform LFSEC 00000071 vulnerabilities and working with Invensys to validate the security update.

Invensys would also 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 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

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).

.