Invensys Operations Management Security Bulletin

Title

InTouch 10 DLL Hijack (LFSEC00000073)

Rating

Medium

Published By

Invensys Operations Management Security Response Center

Update – September 11th, 2012

A bug was discovered in the security updates released on June 13th 2012, and August 1st 2012. The bug causes View to crash under certain conditions. The prior versions had an installation filename **LFSEC0073_20120614.exe** or **LFSEC0073_20100801.exe**.

If you have installed either version, this situation is easily remedied by doing the following.

- Please download the latest version with the installation filename **LFSEC0073_20120910.exe**.
- Uninstall any previous versions using the procedure found in the readme file.
- Install this latest version.

Overview

A *vulnerability* has been discovered in wwClintF.dll, a common component used by InTouch and other Wonderware System Platform products. This vulnerability, if exploited, could result in an attacker creating a back door into the system. The rating is medium as determined by the IOM R&D Security Team and would require the attacker to gain administrative access to the vulnerable node either through social engineering or by other means of local coercion. 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 a software update available to customers that has been tested on all supported versions of:

- InTouch: Window Maker, Window Viewer, InTouch.exe, HistData, Alarm Logger Mgr, Alarm Purge, Alarm DB Restore, Alarm Hist Migration
- App Server – System components, DDE-SuiteLink Objects, aaCalWrapper.exe
- Wonderware Historian,
- InBatch, - Data Access components
- WIS (Server Only), RDB Handler, WCF MX Provider
- DAServers,
- FCS
- FCS SCADA

Recommendations

Customers using versions of the products listed above with the vulnerability SHOULD apply the security update to all nodes where the products are installed. Installation does not require a reboot but will required the shutdown of the associated products that use the component.

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 5.2. 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]

[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
InTouch 2012 and all prior versions	Windows XP, Windows Vista, Windows 7, Windows	5.2	Medium-High	InTouch 10 DLL Hijack (LFSEC00000073-20100910)
Wonderware Application Server 2012 and Prior versions	Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows 2008, Windows 2008 R2	5.2	Medium-High	InTouch 10 DLL Hijack (LFSEC00000073-20100910)
Wonderware Information Server 4.5 and Prior versions	Windows Server 2003, Windows 2008, Windows 2008 R2	5.2	Medium-High	InTouch 10 DLL Hijack (LFSEC00000073-20100910)
InFusion (FCS) 3.5 and Prior versions	Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows 2008, Windows 2008 R2	5.2	Medium-High	InTouch 10 DLL Hijack (LFSEC00000073-20100910)
InBatch 9.5 and all prior versions	Server 2003, Windows 2008, Windows 2008 R2	5.2	Medium-High	InTouch 10 DLL Hijack (LFSEC00000073-20100910)
InFusion SCADA 3.5 and all prior versions	Server 2003, Windows 2008, Windows 2008 R2	5.2	Medium-High	InTouch 10 DLL Hijack (LFSEC00000073-20100910)

Non-Affected Products

- Historian Clients
- Wonderware Information Server Clients
- Wonderware Intelligence Clients

Background

Wonderware is the market leader in real-time operations management software and InTouch is their flagship Human Machine Interface. Wonderware System Platform and InFusion (FCS) 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. Wonderware InBatch provides flexible batch management capabilities. The InBatch

[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.

server component manages the execution of batches and related recipes in a structured way in coordination with controllers and User Interface.

Vulnerability Characterization

The WWClintF DLL contains a vulnerability that may allow an attacker to perform DLL Hijacking which under certain circumstances could lead to an unintended recognizance of the end user's machine. DLL Hijacking is an attack by which malicious code is injected into an application via a call to a malicious DLL with the same name as that used by the application. This type of vulnerability is usually given a lower rating due to the fact that the attacker must have been granted administrative access to the machine a priori meaning the machine may have already been compromised by a previous assault. However, the significance of this type of vulnerability should not be ignored as this is an avenue used by attackers to gain remote access at a later time than when the machine was originally compromised creating a virtual back door into the system.

Update Information

Any machine where the WWClintF DLL is installed is affected and must be patched. No other components of the Wonderware installed products are affected. A reboot is not required. Install the Security Update using instructions provided in the ReadMe for the product and component being installed. In general, the user SHOULD:

- Read the installation instructions provided with the patch
- Shut down any of the affected products
- Install the update
- Restart the products

Please note that the same sequence applies to the uninstall of the update.

Other Information

Acknowledgments

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

Independent Cyber Researcher, Carlos M. Penagos Hollman for reporting the InTouch 10 DLL Hijacking Vulnerability to Invensys (LFSec00000073). Invensys would also like to acknowledge the continued collaboration with ICS-CERT for their expert help in the coordination of 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 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).

.