Invensys Operations Management Security Bulletin

Title

Weak Encryption for InTouch Passwords (LFSEC00000080)

Rating

Medium Low

Published By

Invensys Operations Management Security Response Center

Overview

A *vulnerability* has been discovered in the password storage mechanism for the "**InTouch**" Security Type. **Not** affected by this vulnerability are end users who have chosen "Windows Integrated" security for their InTouch applications rather than the "InTouch" option. This vulnerability, if exploited, could result in an attacker reversing the encryption to obtain the passwords configured for the InTouch application users. The rating is medium low, as determined by the Invensys Operations Management R&D Security Team. It would require the attacker to gain local 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 software updates that have been tested on all supported versions of Wonderware InTouch. These are listed in the table below in the Affected Products and Components section and are now available to customers on the Wonderware Security Central site.

Recommendations

Customers using the following product versions in combination with the InTouch type security SHOULD switch their applications to use Windows Integrated security OR backup their InTouch application off node and then apply the security update to all nodes where the application is deployed. Installation of the Security Update does not require a reboot although all Wonderware applications on the node will need to be shut down. They can be restarted immediately after the patch is installed.

Important: If the application is set up as a Distributed NAD type, then the master node needs to be updated ***last*** after updating all deployed clients. If the application is ArchestrA based, then the IDE node should be updated ***last*** following the update of all the deployed clients.

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 gives this vulnerability an Overall CVSS Score of 5. To review the assessment, use this link: National Vulnerability Database Calculator for LFSEC00000080. 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) using the links embedded in the table below.

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Update
InTouch 2012 R2	Windows XP, Windows Vista, Windows 7	5.0	Medium-Low	Weak Encryption for InTouch Passwords (LFSEC00000080)
InTouch 2012 Patch 01	Windows XP, Windows Vista, Windows 7	5.0	Medium-Low	Weak Encryption for InTouch Passwords (LFSEC00000080)
InTouch 10.1 SP3 Patch 01	Windows XP, Windows Vista, Windows 7	5.0	Medium-Low	Weak Encryption for InTouch Passwords (LFSEC00000080)

Non-Affected Products

- Wonderware Historian and Clients
- Wonderware Information Server and Clients
- Wonderware Intelligence Server and Clients
- Wonderware Application Server
- Wonderware MES
- Wonderware InBatch

Background

Wonderware is the market leader in real-time operations management software and InTouch is their flagship Human Machine Interface (HMI) used for designing, building, deploying and maintaining standardized applications for manufacturing and infrastructure operations.

[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 (12/11/2012)

Cyber-Researchers Seth Bromberger and Slade Griffin discovered the weak password encryption vulnerability while investigating an issue with the Siemens/Moore ProcessSuite application which was built on top of InTouch 7.11. While these products are out of support from both companies and run on Windows 2000, the only option to fix this vulnerability is to migrate the HMI and the OS to versions currently supported, and then install this Security Update. Please consult with Wonderware Tech Support for help with the migration.

Vulnerability Characterization

The InTouch security (type) sub-system contains a vulnerability that may allow an attacker to reverse the encryption of user passwords. This vulnerability cannot be exploited remotely or without user interaction and 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 that could be used by attackers to perform actions on a control system under the account of a legitimate user.

Update Information

Any InTouch application that uses the InTouch security option is affected and must be patched. Applications that use Windows Integrated security or ArchestrA security are not affected. No other Wonderware installed products are affected. A reboot is not required. Install the Security Update using instructions provided in the ReadMe for the version of the product affected. In general, the user SHOULD:

- Read the installation instructions provided with the patch
- Shut down all Wonderware applications on the affected node
- Back up all InTouch applications off node
- Install the update
- Restart the products

The update is reversible if desired. However, the application must be restored from the backup following execution of the uninstall procedure (refer to ReadMe).

Other Information

Acknowledgments

Invensys thanks Seth Bromberger, Principal at NCI Security LLC and Slade Griffin, independent security researcher for their responsible disclosure of the Weak Encryption for InTouch Passwords (LFSec00000080) vulnerability and for validating that the Wonderware InTouch Security Update resolves this issue.

Invensys also appreciates the collaboration of Siemens ProductCERT with the Invensys Operations Management Security Response Center.

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. (Login required)

Invensys Operations Management Security Central

For the latest security information and events, visit Security Central. (Note that this site requires a login account.)

.

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).