# Invensys Wonderware Security Bulletin

## Title

Invensys Wonderware InTouch Improper Input Validation Vulnerability **(LFSEC00000081)**

## Rating

High

## Published By

Invensys R&D Security Response Center

## Overview

Positive Technologies have discovered a *vulnerability* in the InTouch 2012 R2 HMI product which exists in all previous versions. This vulnerability, if exploited, could allow attackers to access local resources (files and internal resources) or enable denial of service attacks. The rating is **High** 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 update availability to customers. The update has been tested on InTouch 2012 R2 (Version 10.6) and is included in System Platform 2012 R2 Patch 01.

## Recommendations

Customers using version 2012 R2 of Wonderware InTouch SHOULD apply System Platform 2012 R2 Patch 01. All earlier versions should apply the mitigations listed below.

**Note:** FCS, InFusion, and InFusion SCADA customers use earlier versions of InTouch, and should also refer to the mitigation section.

Please contact Wonderware tech support if you need assistance.

## 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 (Critical). Details about this scoring system can be found here: http://nvd.nist.gov/cvss.cfm

R&D assessment of this vulnerability using the CVSS Version 2.0 calculator gives this issue an Overall CVSS Score of 6.3. To review the assessment, use this link: National Vulnerability Database Calculator for LFSEC00000081 . 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 | 6.3 | Medium-Low | WW-ASP2012R2-P01 (LFSEC00000081) |
| InTouch 2012 Patch 01 | Windows XP, Windows Vista, Windows 7 | 6.3 | Medium-Low | See Mitigations |
| InTouch earlier versions | Windows XP, Windows Vista, Windows 7 | 6.3 | Medium-Low | See Mitigations |
| FCS, InFusion, and InFusion SCADA – All versions | Windows XP, Windows 7 | 6.3 | Medium-Low | See Mitigations |

## Non-Affected Products

- Wonderware Historian Clients
- Wonderware Information Server and Clients (earlier Security Update Released)
- Wonderware Intelligence Server and Clients
- 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.

## Vulnerability Characterization

InTouch contains a vulnerability that may allow access to local files and other internal resources by exploiting improper parsing of XML external entities in an unsecure deployment[4]. If an attacker manages to make a victim open a project that contains specially crafted XML, InTouch may automatically send the contents of local or remote resource to the attacker's server. It also makes possible to conduct denial of service attacks.

[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.

Any machine that has InTouch 2012 R2 installed is affected and must be patched using the System Platform 2012 R2 Patch 01 described in the ReadMe.

### Update Information

On nodes with InTouch 2012 R2, install the System Platform 2012 R2 Patch 01 using instructions provided in the ReadMe for the product and component being installed. The Security Update for LFSEC00000081 is included in the System Platform 2012 R2 Patch 01 and is the only way to receive the Security Update. For all other previous versions of these products please see the Mitigations section.

### Mitigations

Invensys has developed an update to the InTouch HMI software that mitigates the XML Entity Injection vulnerability. The Positive Technologies Research Team has tested the update and validated that it fixes the vulnerability. Instructions and a link to the update are found at:
https://wdn.wonderware.com/sites/WDN/Pages/Security%20Central/CyberSecurityUpdates.aspx

According to Invensys, any machine running one or more of the products listed above is affected and should be patched. No other components of the Wonderware installed products are affected. Users should upgrade older versions to the InTouch 2012 R2 release and install System Platform 2012 R2 Patch 01 using instructions provided in the ReadMe file for the product and component being installed. Invensys recommends that users:

• Read the installation instructions provided with the patch.

• Shut down any of the affected software products.

• Install the update.

• Restart the software.

For FCS customers, the upgrade to Foxboro Evo Control HMI will include System Platform 2012 R2 Patch 01 as part of the standard installation process. No patch is required with Foxboro Evo Control HMI.

Invensys and ICS-CERT recommend implementing the following defensive measures to protect against this vulnerability and other cyber security risks. This is the recommend mitigation strategy, regardless of whether asset owners can or cannot upgrade to InTouch 2012 R2 Patch 01.

> • Minimize network exposure for all control system devices. Critical devices should not directly face the Internet and there should be no outbound connections from the control system LAN that allow resolution to undefined (non-whitelisted) Internet endpoints.
>
> • Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
>
> • When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion Detection and Mitigation Strategies that is available for download from the ICS-CERT Web page (www.ics-cert.org).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

## Existence Of Exploit

No known public exploits specifically target this vulnerability.

## Other Information

### Acknowledgments

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

Gleb Gritsai, Nikita Mikhalevsky, Timur Yunusov, Denis Baranov, Ilya Karpov, Vyacheslav Egoshin, Dmitry Serebryannikov, Alexey Osipov, Ivan Poliyanchuk, and Evgeny Ermakov of the Positive Technologies Research Team for reporting “INVENSYS WONDERWARE INTOUCH IMPROPER INPUT VALIDATION VULNERABILITY (LFSec00000081)”.

Invensys would also like to acknowledge the continued collaboration with ICS-CERT for their expert help in the coordination of this Security Bulletin and mitigation for this vulnerability.

## Support

For information on how to reach Invensys 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 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 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).