Invensys Operations Management Security Bulletin

Title

Improper Input Validation in Ruby on Rails can result in complete take over on the Dashboard Server node (Tableau Server) host machine shipping with Wonderware Intelligence.

(LFSEC00000090)

Rating

High

Published By

Invensys Operations Management Security Response Center

Update

May 2013: Tableau Server **Version 8 and later** addresses the vulnerabilities outlined in this Security Bulletin. You can either:

- Click here to upgrade.
- Proceed to the Security Updates for versions 7.0.5 through 7.0.12 (following section).

Overview

Multiple vulnerabilities have been discovered in Ruby on Rails which is used in the Tableau Server Software components distributed with Wonderware Intelligence Software versions up to version 1.5 SP1. These vulnerabilities, if exploited, allows remote attackers to bypass intended database-query restrictions which can result in complete take over on the host machine. The rating is High.
This security bulletin announces the software updates available to customers that have been tested on Wonderware Intelligence 1.5 SP1.

For detailed information about the Ruby On Rails vulnerabilities please refer to the following links:

CVE-2013-0155, CVE2013-0156, and CVE-2013-0333

Recommendations

Customers using any version of Wonderware Intelligence up to 1.5 SP1 (with or without LFSec00000089) SHOULD apply the security update to all nodes where the Tableau Dashboard Server is installed.The process consists of un-installing the Dashboard Server and installing the new version. The Server configuration and published dashboards will be preserved during the installation of the new version. If a customer is currently using a version older than 1.5 SP1, a new license is required. Customer can contact their distributor for a new license.

Although not affected by this vulnerability we also recommend the upgade of the Analytics Client nodes, to keep those components to the same synchronised versions.

No reboot should be required after these upgrades.

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

The assessment of the vulnerabilities using the CVSS Version 2.0 calculator based on Invensys' deployment environment of Wonderware Intelligence software rates CVSS Scores is as follows:

- Wonderware Intelligence 1.5 SP1: Overall CVSS Score of 10. A detailed CVSS assessment can be found at the following link.
- Wonderware Intelligence 1.5 SP1 with LFSec000000089: Overall CVSS Score of 7.5. A detailed CVSS assessment can be found at the following link.

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) using the links embedded in the table below.

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Update
Tableau Server of Wonderware Intelligence up to 1.5 SP1 (that corresponds to Tableau Server version up to 7.0.5)	Windows Server 2003, 2003 R2, 2008, 2008 R2 also well as XP, Vista and 7	Remode Code Execution; disclosure of information; unauthorized modification and disruption of service	10	Tableau Ruby on Rails (LFSEC00000090)
Tableau Server of Wonderware Intelligence up to 1.5 SP1+LFSec089 (that corresponds to Tableau Server version up to 7.0.12)	Windows Server 2003, 2003 R2, 2008, 2008 R2 also well as XP, Vista and 7	Remode Code Execution; disclosure of information; unauthorized modification and disruption of service	7.5	Tableau Ruby on Rails (LFSEC00000090)

Non-Affected Products

- N/A

Background

Wonderware Intelligence Software enables user to gather, store, and report on both historical and real-time operational data, using a dashboard to present Key Performance Indicators that are used to visualize, tune and maximize your operations.

Intelligence's Data Model is the foundation for transforming data into actionable information by adding context (equipment, product, work orders, material, personnel, etc.). This data in context helps users to answer Operational questions.

Vulnerability Characterization

The Tableau Server Software components delivered with Wonderware Intelligence Software contain a vulnerability that may allow unauthorized disclosure of information; unauthorized modification and disruption of service in an unsecure deployment[4]. This vulnerability is characterized as *CWE-20 (Improper Input Validation)* that results in SQL Injection attacks. This vulnerability, if exploited, allows

[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.
[4] Any control system installation which does not follow the practices describe in the Invensys Secure Deployment Guide

remote attackers to bypass intended database-query restrictions which can result in complete take over on the host machine

Update Information

Any machine where the Tableau Server Software components from the Wonderware Intelligence Software are installed on is affected and must be upgraded. No other components of Wonderware Intelligence are affected.

Install the Security Update using instructions provided in the ReadMe for the product and component being installed. In general, the user SHOULD uninstall the older Tableau Server Version and install the newer one.

Other Information

Acknowledgments

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

- Tableau Software
- ICS-Cert

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. (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).

.