Invensys Operations Management Security Bulletin

Title

Memory corruption and XXS Vulnerabilities in Wonderware HMI Reports

LFSEC00000059-61

Rating

High

Published By

Invensys Operations Management Security Response Center

Overview

Independent security researchers Billy Rios and Terry McCorkle have discovered memory corruption and cross site scripting vulnerabilities in Wonderware HMI Reports 3.42.835.0304. These vulnerabilities, if exploited, could allow an attacker to compromise the host machine. The rating is high but requires 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 that the software patch is available to customers using all released levels of HMI Reports 3.4.

Recommendations

Customers using versions of HMI Reports 3.4 SHOULD upgrade all nodes where the HMI Reports software is installed. This is a free upgrade to all existing customers of the HMI Reports 3.4 product.

Security vulnerabilities identified in this Bulletin are resolved in future releases.

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 6.0. To review the assessment, use this link: National Vulnerability Database Calculator for LFSEC00000059-61. 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 Infusion Technical Support websites using the links embedded in the table below.

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Update
HMI Reports 3.4	Windows	High	6.0	Wonderware Quick Reports Security Update LFSEC00000059-61

Non-Affected Products

- Quick Reports 2012 (4.0, aka HMI Reports 4.0)

Background

Wonderware is a brand offering of the Operations Management Division of Invensys. Invensys Operations Management is a provider of automation and information technologies and systems.

Vulnerability Characterization

The Wonderware HMI Reports contains memory corruption and cross site scripting vulnerabilities. An attacker would need to create a specially crafted file for the client to open. Successfully exploiting the vulnerability could allow remote code execution in an affected client. Additionally a successful exploit of the XXS vulnerability could allow an attacker to bypass access controls.

These vulnerabilities are remotely exploitable. User interaction is likely required for exploit as users must open a malicious file on a client with the HMI Reports software installed or click on a link to a malicious site while logged into HMI Reports.

Any machine that the HMI Reports software is installed on is affected and must be patched.

[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 Information

Install the Security Update using instructions provided in the ReadMe for the product and component being installed. In general, you SHOULD download the update, the associated upgrade instructions, and the license file update. After installation, you must migrate your report definitions into the new Quick Reports 2012 format, as explained in the upgrade instructions. You must also request a permanent license file from your distributor.

Other Information

Acknowledgments

Invensys thanks the following for the discovery and collaboration with us on these vulnerabilities:

Independent security researchers Billy Rios and Terry McCorkle for reporting the “Memory Corruption and XXS Vulnerabilities in Wonderware HMI reports LFSEC00000059-61” and the continued support and collaboration with 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.

.

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).

.