Invensys Operations Management Security Bulletin

Title

Wonderware Archestra ConfigurationAccessComponent ActiveX Stack Overflow (LFSEC00000037)

Rating

Medium

Published By

IOM Security Response Center

Overview

A *vulnerability* has been discovered in a component used by the Wonderware Archestra IDE (Integrated Development Environment) and the InFusion IEE (Integrated Engineering Environment) in all supported versions of ArchestrA and InFusion with exception of the latest, Wonderware Application Server 3.1 Service Pack 2 Patch 01 (WAS 3.1 SP2 P01). This vulnerability, if exploited, could allow remote code execution. The rating is **medium** and would require social engineering to exploit. Social engineering is the act of manipulating people to unknowingly perform certain actions that may be detrimental to the system. For example, tricking a user to click on an email link or download a file.

This security bulletin announces the software updates available to customers that have been tested on the latest service packs and patches of each major version impacted.

Recommendations

Customers using versions of Wonderware Application Server prior to version 3.1 SP2 P01 SHOULD apply the security update to all nodes where the ArchestrA IDE or InFusion IEE is installed. Installation does not require a reboot and runtime execution is not affected.

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. To review the assessment, use this link: National Vulnerability Database Calculator for LFSEC00000037. 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 Download
IAS 2.1 (all versions) - IDE	Windows XP SP3, Windows 2003	Remote Code Execution	Medium	Industrial Application Server 2.1 Patch02 Security Update LFSEC00000037
WAS 3.0 (all versions) - IDE	Windows XP SP3, Windows 2003, Windows Vista	Remote Code Execution	Medium	Wonderware Application Server 3.0 SP2 Security Update LFSEC00000037
WAS 3.1 (all versions) - IDE	Windows XP SP3, Windows 2003, Windows Vista, Windows 2008	Remote Code Execution	Medium	Wonderware Application Server 3.1 Security Update LFSEC00000037; Wonderware Application Server 3.1 SP1 Security Update LFSEC00000037
InFusion CE 1.0 (all versions[4]) – IEE	Windows XP SP3, Windows 2003	Remote Code Execution	Medium	Industrial Application Server 2.5 Security Update LFSEC00000037
InFusion CE 2.0 - IEE	Windows XP SP3, Windows 2003	Remote Code Execution	Medium	Wonderware Application Server 3.1 SP1 Security Update LFSEC00000037
InFusion FE 1.0 (all versions[5]) - IEE	Windows XP SP3, Windows 2003	Remote Code Execution	Medium	Industrial Application Server 2.5 Security Update LFSEC00000037
InFusion FE 2.0 - IEE	Windows XP SP3, Windows 2003, Windows Vista, Windows 2008	Remote Code Execution	Medium	Wonderware Application Server 3.1 Security Update LFSEC00000037
InFusion SCADA 2.0 – IEE	Windows XP SP3, Windows 2003, Windows Vista, Windows 2008	Remote Code Execution	Medium	Wonderware Application Server 3.1 Security Update LFSEC00000037

Background

[2] 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] Infusion Control Edition 1.0 (all versions) refers to Infusion Control Edition 1.0, 1.1 (and all service packs), 1.2, 1.2.1 and 1.2.2.
[5] Infusion Foundation Edition 1.0 (all versions) refers to Infusion Foundation Edition 1.0 and Infusion Foundation Edition 1.0.1.

The Archestra IDE and InFusion IEE interface with the galaxy repository to create, edit, and deploy application objects. The IDE is usually found only on development nodes. Please note that for InFusion Control Edition, the IEE is typically installed on all workstations, and that this security patch affects IEE workstations both on and off the MESH network.

Vulnerability Characterization

The Archestra IDE and InFusion IEE contain a vulnerability that MAY allow remote code execution in an unsecure deployment[6]. On a machine with the IDE or IEE installed, the vulnerability could be exploited by executing a malicious email attachment on the IDE or IEE node.

All machines on which the IDE or IEE is installed are affected and MUST be patched. No other components of InTouch, InFusion or Wonderware Application Server are affected. No reboot is required. There are two requirements for installing the security update:

- The installing user MUST be an Administrator.
- The IDE or IEE MUST be closed.

Note that the Security Update can be uninstalled.

Update Information

Install the Security Update using instructions provided in the ReadMe for the product and component being installed. In general, the user SHOULD close the IDE or IEE and be an Administrator to install the Security Update. A reboot is not required.

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

Other Information

Acknowledgments

Invensys thanks the following for the discovery and subsequent collaboration with us to investigate and remedy this vulnerability:

Richard van Eeden of IOActive Labs for reporting the Wonderware Archestra ConfigurationAccessComponent ActiveX Stack Overflow (LFSEC00000037).

Support

For information on how to reach IOM 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.

IOM Cyber Security Updates

For information and useful links related to security updates, please visit the IOM 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 IOM Security Central.

Disclaimer