Date: 06/30/2017

Wonderware Security Bulletin LFSEC00000116

Title

Wonderware ArchestrA Logger multiple vulnerabilities

Rating

High

Published By

Wonderware|Schneider Electric Security Response Center

Overview

Wonderware by Schneider Electric has created a security update to address vulnerabilities in the **Wonderware ArchestrA Logger versions 2017.426.2307.1 or prior**. The vulnerabilities, if exploited, could allow a malicious entity to remotely execute arbitrary code or cause denial of service.

Schneider Electric recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

This security bulletin announces the software security update for the **Wonderware ArchestrA Logger version 2017.426.2307.1 or prior.**

Recommendations

Customers using any Wonderware, Avantis, SimSci, or Skelta product that installs the **Wonderware ArchestrA Logger version 2017.426.2307.1 or prior** are affected and should apply the **Wonderware ArchestrA Logger Security Patch v2017.517.2328.1** as soon as possible.

Background

The Wonderware ArchestrA Logger is a common component providing logging capabilities to products from Wonderware, Avantis, SimSci, and Skelta. These products are used in many industries worldwide, including manufacturing, energy, food and beverage, chemical, and water and wastewater management.

To identify if the Wonderware ArchestrA Logger is installed and its version, navigate to “Program Files (x86)\Common Files\ArchestrA” and look for “aaLogger.exe”. If the file is present, then you have installed a product that uses the Wonderware ArchestrA Logger component. Right click on the aaLogger.exe, choose properties, then details; if the file version is 2017.426.2307.1 or prior then you are using a vulnerable version.

Vulnerability Details

The Wonderware ArchestrA Logger component exposes an RPC interface for remote management. Some of the methods on this interface are susceptible to:

1) Remote Code Execution, which could allow an attacker to run arbitrary code in the context of a highly privileged account.
2) Memory Leaks, which could allow an attacker to exhaust the memory of the target machine and cause Denial of Service for applications running on the target machine.
3) Null Pointer Dereferences, which could allow an attacker to crash the logger process causing Denial of Service for logging and log-viewing operations. Note that applications which use the Wonderware ArchestrA Logger continue to run when the Wonderware ArchestrA Logger service is unavailable and will function correctly, losing only the ability to log.

Security Update

The following Security Update addresses the vulnerabilities outlined in this Security Bulletin.
June 30, 2017: Wonderware ArchestrA Logger Security Patch 2017.517.2328.1

Affected Products, Components, and Corrective Security Patches

The following table identifies the currently supported products affected. Software updates can be downloaded from the Global Customer Support “Software Download” area or from the links below:

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Security Update
Wonderware ArchestrA Logger 2017.426.2307.1 or prior	Multiple	Confidentiality, Integrity, Availability	High	https://gcsresource.invensys.com/tracking/ConfirmDownload.aspx?id=22429

Vulnerability Characterization and CVSSv3 Rating

CWE-121: Stack-based buffer overflow, CWE-400: Uncontrolled resource consumption, CWE-476: Null pointer dereference

ArchestrA Logger RCE	**9.8** | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
ArchestrA Logger Leak	**8.6** | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
ArchestrA Logger Crash	**7.5** | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Acknowledgements

Schneider Electric would like to thank:

- **Andrey Zhukov** from **USSC** for the discovery, responsible disclosure of this vulnerability, and verification of the security patch.
- **ICS-Cert** for coordination of advisories

Support

For information on how to reach Schneider Electric support for your product, please refer to this link: Schneider Electric Software Global Customer Support.

If you discover errors or omissions in this Security Notification, please report the finding to Support.

Wonderware Security Central

For the latest security information and security updates, please visit Security Central.

Cyber Security Standards and Best Practices

For information regarding how to secure Industrial Control Systems please reference NIST SP800-82r2.

NVD Common Vulnerability Scoring System (CVSS v3)

The U.S. Department of Homeland Security has adopted the common Vulnerability Scoring System (CVSS v3) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v3 produces a numerical score as well as a textual representation of that score reflecting the severity of a vulnerability. Scores range from 0.0 (no impact) to a maximum of 10.0 (critical impact with minimal effort to exploit). For additional information please refer to the CVSSv3 specifications.

Disclaimer

THE INFORMATION PROVIDED HEREIN IS PROVIDED “AS-IS” AND WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC AND ITS AFFILIATES, PARENT AND SUBSIDIARIES (COLLECTIVELY, “SCHNEIDER ELECTRIC”) DISCLAIM 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 SCHNEIDER ELECTRIC, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES WILL CREATE A WARRANTY AND CUSTOMER MAY NOT RELY ON ANY SUCH INFORMATION OR ADVICE.

SCHNEIDER ELECTRIC DOES NOT WARRANT THAT THE SOFTWARE WILL MEET CUSTOMER’S REQUIREMENTS, THAT THE SOFTWARE WILL OPERATE IN COMBINATIONS OTHER THAN AS SPECIFIED IN SCHNEIDER ELECTRIC’S DOCUMENTATION OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

IN NO EVENT WILL SCHNEIDER ELECTRIC 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 SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC’S 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 ONE HUNDRED DOLLARS ($100 USD).