



AVEVA Security Bulletin LFSEC00000129

Title

Wonderware License Server Insecure 3rd Party component usage

Rating

Critical

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. (“AVEVA”) has created a security update to address an outdated and insecure 3rd party component used in:

- **Wonderware License Server 4.0.13100 and older**

The vulnerability, if exploited, could result in remote code execution with administrative privileges. Wonderware License Server is delivered by **Wonderware Information Server 4.0 SP1 and older** and **Historian Client 2014 R2 SP1 P02 and older**.

Recommendations

Customers using the Counted Licenses feature with “ArchestrAServer.lic” in **Wonderware License Server 4.0.13100 or older** are affected and should apply **Hotfix Wonderware License Server VU-485744**.

Vulnerability Details, Characterization, and CVSSv3 Rating

The vulnerability exists in Flexera Imgrd v11.13.1.1 and older, a 3rd party component used by Wonderware License Server. Please refer to Flexera [VU-485744](#) for further details.

Security Update

The following Security Update addresses the vulnerability outlined in this Security Bulletin:

July 20, 2018: Hotfix Wonderware License Server VU-485744

Software Security Update Download:

<https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=5076>

Acknowledgements

AVEVA would like to thank:

- **ICS-Cert** for coordination of advisories



Support

For information on how to reach AVEVA support for your product, please refer to this link: [AVEVA Software Global Customer Support](#).

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

AVEVA 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. AVEVA AND ITS AFFILIATES, PARENT AND SUBSIDIARIES 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 AVEVA, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES WILL CREATE A WARRANTY AND CUSTOMER MAY NOT RELY ON ANY SUCH INFORMATION OR ADVICE.

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

IN NO EVENT WILL AVEVA 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 AVEVA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. AVEVA'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).