DATE: 01/31/2024

SECURITY BULLETIN AVEVA-2024-002

Title

Uncontrolled Search Path Element vulnerability in AVEVA Edge (formerly known as InduSoft Web Studio)

Rating

High

Published By

AVEVA Software Security Response Center

Overview

AVEVA Group Limited on behalf of itself and its subsidiaries ("AVEVA") has created a security update to address vulnerabilities in AVEVA Edge 2020 R2 SP2 and all prior versions (formerly known as InduSoft Web Studio).

Vulnerability Technical Details

1. Uncontrolled Search Path Element

The vulnerability, if exploited, could allow a malicious entity with access to the file system to achieve arbitrary code execution and privilege escalation by manipulating AVEVA Edge to load an unsafe DLL.

CWE-427 Uncontrolled Search Path Element
CVSS v3.1: **7.3** | AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
CVE-2023-6132

Recommendations

AVEVA recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

Customers using AVEVA Edge 2020 R2 SP2 and all prior versions (formerly known as InduSoft Web Studio) are affected and should upgrade to AVEVA Edge 2023, or AVEVA Edge 2020 R2 SP2 P01 as soon as possible.

In addition to applying the security fix, the following general precautions should be taken throughout the lifetime of AVEVA Edge projects:

- Access Control Lists should be applied to all folders where users will save and load project files.
- Maintain a trusted chain-of-custody on project files during creation, modification, distribution, and use.
- Train users to always verify the source of a project is trusted before opening or executing it.

Downloads

- AVEVA Edge 2023:
  https://softwaresupportsp.aveva.com/#/producthub/details?id=0c8abaf3-2e4c-4be1-aa78-3ad445c58a16
- AVEVA Edge 2020 R2 SP2 P01:
  https://softwaresupportsp.aveva.com/#/producthub/details?id=1e5d9950-d945-4bab-984b-245fe3f152ac

Acknowledgements

AVEVA would like to thank:

- **ADLab of Venustech** and **Ting Chen of UESTC** for the discovery and responsible disclosure of this vulnerability
- **CISA** for coordination of advisories

Support

For information on how to reach AVEVA support for your product, please refer to this link: AVEVA Customer Support.
If you discover errors or omissions in this Security Notification, please report the finding to Support.

AVEVA Security Central

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

U.S. Department of Commerce Industrial Control Systems Security Guide

For general information regarding how to secure Industrial Control Systems please reference the NIST Guide to Operational Technology (OT) Security, NIST SP800-82r3.

NVD Common Vulnerability Scoring System (CVSS v3.1)

The U.S. Department of Homeland Security has adopted the Common Vulnerability Scoring System (CVSS v3.1) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v3.1 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 CVSS v3.1 specifications.

Coordination with Authorities

Organizations observing suspected malicious activity should follow established internal procedures and report findings to applicable authorities for tracking and correlation against other incidents.

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 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 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).