DATE: 08/18/2022

SECURITY BULLETIN AVEVA-2022-005

Title

Multiple vulnerabilities in AVEVA Edge (formerly known as InduSoft Web Studio)

Rating

High

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. ("AVEVA") has created a security update to address vulnerabilities in AVEVA Edge 2020 R2 SP1 and all prior versions (formerly known as InduSoft Web Studio). The vulnerabilities, if exploited, could result in arbitrary code execution, information disclosure, or denial of service.

Vulnerability Technical Details

1. Unsafe Deserialization

The vulnerability, if exploited, could allow a malicious entity who tampers with project files to achieve arbitrary code execution in AVEVA Edge.

CWE-502: Deserialization of Untrusted Data
CVSS v3.1: **7.8** | AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVE-2022-28685

2. 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 tricking AVEVA Edge to load an unsafe DLL.

CWE-427 Uncontrolled Search Path Element
CVSS v3.1: **7.8** | AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-28686, CVE-2022-28687, CVE-2022-28688

3. Improper Restriction of XML External Entity Reference

The vulnerability, if exploited, could allow a malicious entity to cause a Denial of Service on AVEVA Edge or to extract arbitrary files from the host machine on which AVEVA Edge is running.

CWE-611: Improper Restriction of XML External Entity Reference
CVSS v3.1: **6.6 Medium** | AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H
CVE-2022-36969

4. Insufficient UI Warning of Dangerous Operations

Scripting capability is provided in AVEVA Edge to enable end-user customizations at runtime. The code that can be executed in scripts is intentionally unrestricted. A malicious user could abuse the scripting feature to achieve arbitrary code execution.

CWE-357: Insufficient UI Warning of Dangerous Operations
CVSS v3.1: **7.8** | AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVE-2022-36970

Recommendations

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

Customers using AVEVA Edge 2020 R2 SP1 are affected and should apply HF 2020.2.00.40 as soon as possible.
Customers using AVEVA Edge 2020 R2 and all prior versions (formerly known as InduSoft Web Studio) are affected and should first upgrade to AVEVA Edge 2020 R2 SP1 and then apply HF 2020.2.00.40 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

Starting with HF 2020.2.00.40, AVEVA Edge is introducing the following security enhancements:

- When a user selects a project file to open, a warning will be presented asking the user if the project can be trusted. The choice is remembered per project and applied to future operations.
- Newly created projects will use a safe serialization mechanism. Projects created in HF2020.2.00.40 are not backward compatible with AVEVA Edge 2020 R2 SP1 and all prior versions (formerly known as InduSoft Web Studio).
- Legacy projects that are opened in HF2020.2.00.40 and saved will be migrated to use a safe serialization mechanism. After a project is migrated it will not be backward-compatible with AVEVA Edge 2020 R2 SP1 and all prior versions.

For additional detail please refer to the supplied help file in HF 2020.2.00.40.

Downloads

- AVEVA Edge HF 2020.2.00.40: https://softwaresupportsp.aveva.com/#/producthub/details?id=e1598a96-31e2-4370-c17c-08da7168e83a
- AVEVA Edge 2020 R2 SP1: https://softwaresupportsp.aveva.com/#/producthub/details?id=f03eb16e-2ca0-41a0-8998-08d99cd36dd5

Acknowledgements

AVEVA would like to thank:

- (CVE-2022-28685) **Chris Anastasio** from **Incite Team** for the discovery
- (CVE-2022-28686 and CVE-2022-36969): **Piotr Bazydło** for the discovery
- (CVE-2022-28687): **Pedro Ribeiro** and **Radek Domanski** from **Flashback Team** for the discovery
- (CVE-2022-28688): **Daan Keuper** and **Thijs Alkemade** from **Computest** for the discovery
- (CVE-2022-36970): **Aaron Ferber** for the discovery
- **Trend Micro Zero Day Initiative** for responsible disclosure and coordination of advisories/CVEs
- **ICS-Cert** 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 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 v3.1)

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.

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).