DATE: 11/22/2022

SECURITY BULLETIN AVEVA-2022-006

Title

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

Rating

Critical

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. (“AVEVA”) has created a security update to address vulnerabilities in all versions of AVEVA™ Edge (formerly known as InduSoft Web Studio) up to 2020 R2 SP1 w/ HF 2020.2.00.40. The vulnerabilities, if exploited, could result in arbitrary code execution, information disclosure, or denial of service.

Vulnerability Technical Details

1. Improper Access Control

The vulnerability, if exploited, could allow a malicious entity to execute arbitrary commands with the security context of the StADOSvr.exe process. In most instances this will be a standard-privileged user account under which the AVEVA Edge runtime was started. It is possible for a high-privileged service account to have been configured and assigned for running AVEVA Edge runtime.

CWE-284: Improper Access Control
CVSS v3.1: **9.8 Critical** | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2021-42796

2. Universal Naming Convention (UNC) Path Injection and/or Traversal

The vulnerability, if exploited, could allow a malicious entity to trick the AVEVA Edge runtime into disclosing a Windows access token of the user account configured for accessing external DB resources.

CWE-40: Path Traversal (UNC)
CVSS v3.1: **8.6 High** | AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
CVE-2021-42797

3. Use of vulnerable 3rd party component subject to DLL Hijacking

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 the AVEVA Edge InstallShield package to load an unsafe DLL. This attack is only possible during the installation or when performing an install/repair operation.

CWE-427 Uncontrolled Search Path Element
CVSS v3.1: **7.8 High** | AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2016-2542

4. Exposure of Sensitive Information to an Unauthorized Actor

The vulnerability, if exploited, could allow a malicious entity to probe the internal network.

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
CVSS v3.1**: 5.3 Med** | AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVE-2021-42794

Recommendations

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

Customers using any version of AVEVA™ Edge (formerly known as InduSoft Web Studio) up to 2020 R2 SP1 w/ HF 2020.2.00.40 are affected and should apply AVEVA™ Edge 2020 R2 SP2 as soon as possible.

To further reduce exploitability, apply network and OS firewall rules to protect the AVEVA Edge Database Gateway from unauthorized access. The Database Gateway port is configurable (3997 by default).

Downloads

- AVEVA Edge 2020 R2 SP2: https://softwaresupportsp.aveva.com/#/producthub/details?id=bd805851-0c68-4343-15ee-08da9a4aa617

Acknowledgements

AVEVA would like to thank:

- **Sam Hanson** from **Dragos** for the discovery, responsible disclosure, and retesting of fixes
- **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).