SECURITY BULLETIN AVEVA-2024-002

タイトル

AVEVA Edge（旧称：InduSoft Web Studio）における、制御されていない検索パス要素の脆弱性

評価

高（High）

発行者

AVEVA Software Security Response Center

概要

AVEVA Group Limited は、自社およびその子会社（以下「AVEVA」）を代表して、AVEVA Edge 2020 R2 SP2 およびそれ以前のすべてのバージョン（旧称 InduSoft Web Studio）の脆弱性に対処するためのセキュリティアップデートを作成しました。

脆弱性の技術的詳細

1. 制御されていない検索パス要素

   この脆弱性が悪用されると、標準権限を持つローカル OS 認証ユーザーが、これらの製品がインストールされているマシン上のシステム権限に昇格され、ターゲットマシンが完全に侵害される可能性があります。

   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

推奨事項

AVEVA は、各組織が自社の運用環境、アーキテクチャ、および製品実装に基づいて、この脆弱性の影響を評価することを推奨します。

AVEVA Edge 2020 R2 SP2 およびそれ以前のすべてのバージョン（旧称：InduSoft Web Studio）をご利用のお客様は、影響を受けるため、AVEVA Edge 2023 または AVEVA Edge 2020 R2 SP2 P01 にできるだけ早くアップグレードしてください。

セキュリティ修正プログラムの適用に加え、AVEVA Edge プロジェクトのライフサイクル全体を通して、以下の一般的な予防措置を講じる必要があります。
- ユーザーがプロジェクトファイルを保存および読み込むすべてのフォルダに、アクセス制御リストを適用してください。
- プロジェクトファイルの作成、変更、配布、および使用の過程において、信頼できる管理履歴を維持してください。
- ユーザーがプロジェクトを開いたり実行したりする前に、必ずそのソースが信頼できるものであることを確認するよう、トレーニングを実施してください。

ダウンロード

- AVEVA Edge 2023
- AVEVA Edge 2020 R2 SP2 P01

謝辞

AVEVA からの感謝の意:
- この脆弱性の発見と責任ある開示にご尽力いただいた Venustech の ADLab および UESTC の Ting Chen 氏
- 勧告の調整にご尽力いただいた CISA

サポート

お使いの製品の AVEVA サポートへのアクセス方法については、次のリンクを参照してください:
AVEVA カスタマー サポート
https://www.aveva.com/en/support-and-success/support-contact/
このセキュリティ通知に誤りや脱落を発見した場合は、その結果をサポートに報告してください。

AVEVA セキュリティセントラル

最新のセキュリティ情報とセキュリティ アップデートについては、Security Central にアクセスしてください。https://softwaresupportsp.aveva.com/#/securitycentral

サイバー セキュリティの基準とベスト プラクティス

産業用制御システムを保護する方法については、NIST SP800-82r3 を参照してください。
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

NVD の一般的な脆弱性スコアリング システム(CVSS v3.1)

米国国土安全保障省は、IT 脆弱性の特徴と影響を伝達するためのオープン フレームワークを提供する NVD の一般的な脆弱性スコアリング システム (CVSS v3.1) を採用しました。 CVSS v3.1 は、数値スコアと、脆弱性の重大度を反映するそのスコアのテキスト表現を生成します。 スコアの範囲は 0.0 (影響なし) から最大 10.0 (悪用の労力が最小限である重大な影響) までです。 詳細については、CVSS v3.1 仕様を参照してください。

https://www.first.org/cvss/specification-document

当局との調整

疑わしい悪意のある活動を観察している組織は、確立された内部手順に従い、調査結果を該当する当局に報告して、追跡と他のインシデントとの関連付けを行う必要があります。

免責事項

ここに提供される情報は「現状のまま」提供され、いかなる種類の保証もありません。

AVEVA およびその関連会社、親会社、子会社は、商品性および特定目的への適合性に関する黙示の保証を含むがこれらに限定されない、明示または黙示を問わず、すべての保証を否認します。 AVEVA、そのディーラー、ディストリビューター、代理店、または従業員が提供する口頭または書面による情報またはアドバイスは、保証を作成するものではなく、顧客はそのような情報またはアドバイスに依存することはできません。

AVEVA は、本ソフトウェアがお客様の要件を満たすこと、AVEVA のドキュメントに指定されている以外の組み合わせで本ソフトウェアが動作すること、または本ソフトウェアの動作が中断されないこと、またはエラーがないことを保証しません。

AVEVA またはそのサプライヤー、ディーラー、ディストリビューター、エージェント、または従業員は、いかなる間接的、偶発的、特別、懲罰的、結果的損害、または顧客または第三者が被った利益、収益、データまたは使用の損失に対する損害についても責任を負わないものとします。 たとえ AVEVA がそのような損害の可能性について知らされていたとしても、契約または不法行為に基づく行為であるかどうかにかかわらず、当事者の責任を負いません。 本契約に基づく、または本契約に関連する損害および費用に対する AVEVA の責任 (契約上の行為、不法行為またはその他の行為によるものであるかにかかわらず) は、いかなる場合も 100 ドル (100 米ドル) を超えないものとします。