SECURITY BULLETIN AVEVA-2022-005

タイトル

AVEVA™ Edge (旧称 InduSoft Web Studio) の複数の脆弱性

評価

高（High）

発行者

AVEVA Software Security Response Center

概要

AVEVA Software LLC (「AVEVA」) は、AVEVA Edge 2020 R2 SP1 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更新プログラムを作成しました。 この脆弱性が悪用されると、任意のコードの実行、情報漏えい、またはサービス拒否が発生する可能性があります。

脆弱性の技術的詳細

AVEVA Software Security Response Center

1. 安全でない逆シリアル化
   この脆弱性が悪用されると、プロジェクト ファイルを改ざんする悪意のあるエンティティが AVEVA Edge で任意のコードを実行する可能性があります。

   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. 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、悪意のあるエンティティが AVEVA Edge ランタイムをだまして、外部 DB リソースへのアクセス用に構成されたユーザー アカウントの Windows アクセス トークンを開示させる可能性があります。

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. XML 外部エンティティ参照の不適切な制限
   この脆弱性が悪用されると、悪意のあるエンティティが AVEVA Edge でサービス拒否を引き起こしたり、AVEVA Edge が実行されているホスト マシンから任意のファイルを抽出したりする可能性があります。
   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. 危険な操作の不十分な UI 警告
   スクリプト機能が AVEVA Edge で提供され、実行時にエンド ユーザーのカスタマイズを可能にします。 スクリプトで実行できるコードは、意図的に制限されていません。 悪意のあるユーザーがスクリプト機能を悪用して、任意のコードを実行する可能性があります。
   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

推奨事項

AVEVA は、組織が運用環境、アーキテクチャ、および製品の実装に基づいて、これらの脆弱性の影響を評価することを推奨しています。
AVEVA Edge 2020 R2 SP1 を使用しているお客様は影響を受けるため、できるだけ早く HF 2020.2.00.40 を適用する必要があります。
AVEVA Edge 2020 R2 およびそれ以前のすべてのバージョン (旧称 InduSoft Web Studio) を使用しているお客様は影響を受けるため、まず AVEVA Edge 2020 R2 SP1 にアップグレードしてから、できるだけ早く HF 2020.2.00.40 を適用する必要があります。
セキュリティ修正プログラムの適用に加えて、AVEVA Edge プロジェクトの存続期間中、次の一般的な予防措置を講じる必要があります。
・アクセス制御リストは、ユーザーがプロジェクト ファイルを保存およびロードするすべてのフォルダーに適用する必要があります。
・プロジェクト ファイルの作成、変更、配布、および使用中に、信頼できる一連の管理を維持する
・プロジェクトを開くか実行する前に、プロジェクトのソースが信頼できることを常に確認するようにユー

ザーをトレーニングします。

HF 2020.2.00.40 以降、AVEVA Edge は次のセキュリティ強化を導入しています。

・ユーザーが開くプロジェクト ファイルを選択すると、そのプロジェクトが信頼できるかどうかを尋ねる警告が表示されます。 選択はプロジェクトごとに記憶され、将来の操作に適用されます。

・新しく作成されたプロジェクトは、安全なシリアル化メカニズムを使用します。 HF2020.2.00.40 で作成されたプロジェクトは、AVEVA Edge 2020 R2 SP1 およびそれ以前のすべてのバージョン（旧称 InduSoft Web Studio）と下位互換性がありません。

・HF2020.2.00.40 で開かれて保存されたレガシー プロジェクトは、安全なシリアル化メカニズムを使用するように移行されます。 プロジェクトを移行すると、AVEVA Edge 2020 R2 SP1 およびそれ以前のすべてのバージョンとの下位互換性がなくなります。

詳細については、HF 2020.2.00.40 で提供されているヘルプ ファイルを参照してください。

ダウンロード

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

謝辞

AVEVA からの感謝の意:

・(CVE-2022-28685) Incite Team の Chris Anastasio による発見

・(CVE-2022-28686 および CVE-2022-36969): Piotr Bazydło による発見

・(CVE-2022-28687): Flashback Team の Pedro Ribeiro と Radek Domanski による発見

・(CVE-2022-28688): Computest の Daan Keuper と Thijs Alkemade による発見

・(CVE-2022-36970): Aaron Ferber による発見

・アドバイザリ/CVE の責任ある開示と調整のための Trend Micro Zero Day Initiative

・アドバイザリの調整のための ICS-Cert

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 SP800-82r2 を参照してください。
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.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

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。