SECURITY BULLETIN AVEVA-2022-006

タイトル

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

評価

致命的（Critical）

発行者

AVEVA Software Security Response Center

概要

AVEVA Software LLC (「AVEVA」) は、2020 R2 SP1 w/ HF 2020.2.00.40 までの AVEVA　Edge (旧称 InduSoft Web Studio) のすべてのバージョン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. 不適切なアクセス制御

   この脆弱性が悪用されると、悪意のあるエンティティが StADOSvr.exe プロセスのセキュリティ コンテキストで任意のコマンドを実行する可能性があります。 ほとんどの場合、これは AVEVA Edge ランタイムが開始された標準特権ユーザー アカウントになります。 AVEVA Edge ランタイムを実行するために、高い権限を持つサービス アカウントが構成され、割り当てられている可能性があります。

   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) パス インジェクションおよび/またはトラバーサル

   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-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. DLL ハイジャックの対象となる脆弱なサードパーティ製コンポーネントの使用

   この脆弱性が悪用されると、ファイル システムへのアクセス権を持つ悪意のあるエンティティが、AVEVA Edge InstallShield パッケージをだまして安全でない DLL をロードすることで、任意のコードを実行し、権限を昇格させる可能性があります。 この攻撃は、インストール時またはインストール/修復操作の実行時にのみ可能です。

   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. 無許可のアクターへの機密情報の公開

   この脆弱性が悪用された場合、悪意のあるエンティティが内部ネットワークを調査できる可能性があります。

   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

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。

2020 R2 SP1 HF 2020.2.00.40 までの AVEVA™ Edge (旧称 InduSoft Web Studio) のいずれかのバージョン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 AVEVA™ Edge 2020 R2 SP2 を適用する必要があります。

悪用される可能性をさらに減らすには、ネットワークと OS のファイアウォール ルールを適用して、AVEVA Edge Database Gateway を不正アクセスから保護します。 データベース ゲートウェイ ポートは構成可能です (デフォルトでは 3997)。

ダウンロード

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

謝辞

AVEVA からの感謝の意:
・発見、責任ある開示、および修正の再テストについて、Dragos の Sam Hanson 氏
・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。