# SECURITY ADVISORY AVEVA-2022-001

## タイトル

AVEVA™ InTouch Access Anywhere および AVEVA™ Plant SCADA Access Anywhere – ストリーミングされたアプリから OS コンテキストへのエスケープ

## 評価

高（High）

## 発行者

AVEVA Software Security Response Center

## 概要

AVEVA ソフトウェア LLC (“AVEVA”) は、AVEVA™ InTouch Access Anywhere (すべてのバージョン) および AVEVA™ Plant SCADA Access Anywhere (以前は AVEVA Citect Anywhere および Schneider Electric Citect Anywhere として知られていたすべてのバージョン) と組み合わせて有効にして使用する場合、特定の Windows オペレーティング システム機能をお客様にアドバイスしています。 脆弱性が発生する可能性があります。 この脆弱性が悪用されると、認証されたユーザーがストリーミング アプリケーション (AVEVA™ InTouch Access Anywhere および AVEVA™ Plant SCADA Access Anywhere) のコンテキストから OS に逃げ込み、任意の OS コマンドを起動することができます。 アプリケーションをエスケープしている認証済みユーザーのセキュリティ コンテキストでコマンドが実行されるため、この脆弱性によって特権が昇格されることはありません。

## 背景

Windows OS は、任意のアプリケーションの上に「言語バー」をオーバーレイするように構成できます。この OS 機能が有効になっている場合、OS 言語バー UI は、InTouch Access Anywhere および Plant SCADA Access Anywhere アプリケーションと一緒にブラウザで表示できます。 Windows OS 言語バーを悪用して OS コマンド プロンプトを起動し、アプリケーションから OS へのコンテキスト エスケープを引き起こす可能性があります。

## 緩和策

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、この脆弱性の影響を評価することをお勧めします。

影響を受ける AVEVA 製品を使用しているお客様は、次のことを行う必要があります。

・企業ポリシーで必要な場合を除き、InTouch Access Anywhere および Plant SCADA Access Anywhere アプリケーションをホストするサーバー マシンで Windows 言語バーを無効にします。

・InTouch Access Anywhere および Plant SCADA Access Anywhere アプリケーションのリモート アクセス専用の最小限の権限を持つ一意のユーザー アカウントを作成します。

・OS のグループ ポリシー オブジェクト (GPO) を利用して、これらの一意のユーザー アカウントに許可される操作をさらに制限します。

・Microsoft の推奨ブロック リストに基づいてアクセスを制限します:
https://docs.microsoft.com/enus/windows/security/threat-protection/windows-defender-application-control/microsoftrecommended-block-rules

## 脆弱性の特徴付けと CVSSv3 評価

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、この脆弱性の影響を評価することをお勧めします。

AVEVA™ InTouch Access Anywhere および AVEVA™ Plant SCADA Access Anywhere アプリケーションは OS にエスケープします。

CWE-668 間違った領域へのリソースの露出 7.4 | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L

## 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ついて、Aceaspa の Giovanni Delvecchio に感謝します。

・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。