SECURITY BULLETIN AVEVA-2023-001

タイトル

AVEVA™ InTouch Access Anywhere および AVEVA™ Plant SCADA Access Anywhere: 複数の脆弱性

評価

致命的（Critical）

発行者

AVEVA Software Security Response Center

概要

AVEVA ソフトウェア、LLC。（「AVEVA」）は、以下に影響を与える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。

- AVEVA InTouch Access Anywhere 2023 およびそれ以前のすべてのバージョン。 InTouch Access Anywhere は、スタンドアロン インストールと、AVEVA システム プラットフォームのオプションのサブ機能の両方として提供されます。
- AVEVA Plant SCADA Access Anywhere 2020 R2 およびそれ以前のすべてのバージョン（以前の Citect Anywhere)

脆弱性の技術的詳細

1. 古いバージョンの OpenSSL

   1.1.1q より前のバージョンの OpenSSL は、任意のコードの実行やサービス拒否を引き起こす脆弱性の影響を受けやすくなっています。 OpenSSL の脆弱性とリリース ノートのログは、次の場所にあります。

   https://www.openssl.org/news/vulnerabilities-1.1.1.html

   Highest CVSSv3.1: 9.8 Critical | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   Highest CVE-2021-3711

2. パス・トラバーサル

   この脆弱性が悪用された場合、認証されていないユーザーが、これらの製品が実行されているシステムから任意のファイルをリモートで読み取ることができ、情報漏えいが発生する可能性があります。

   この脆弱性を標的とする公開機能のエクスプロイト コードが存在します。

   CWE-23: Relative Path Traversal

   CVSS v3.1: 7.5 High | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

   CVE-2022-23854

3. 古いバージョンの jQuery

   3.5.0 より前のバージョンの jQuery は、複数の脆弱性の影響を受けます。

   Jquery の変更ログ:

   https://blog.jquery.com/category/jquery/

   Highest CVSSv3.1: 6.1 Medium | AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

   Highest CVE-2020-11022

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。 影響を受ける製品を使用しているお客様は、できるだけ早くセキュリティ更新プログラムを適用する必要があります。

セキュリティ更新プログラムの適用に加えて、次の一般的な予防措置を講じて、Access Anywhere Secure Gateway サービスを強化する必要があります。

・ファイアウォール ルールを適用してネットワークへの露出を減らす

セキュリティ更新プログラムのダウンロード

AVEVA InTouch Access Anywhere

・現在主流でサポートされているすべての影響を受けるバージョンは、古いバージョンをアンインストールしてから AVEVA InTouch Access Anywhere 2023b 以降をインストールすることで修正できます:

https://softwaresupportsp.aveva.com/#/producthub/details?id=d848918b-c3c3-489d-e439-08dace3d2997

注: 古いバージョンのこれらの脆弱性に対するホット フィックスは利用できません。

AVEVA Plant SCADA Access Anywhere

・現在メインストリーム サポートされている影響を受けるすべてのバージョンは、古いバージョンをアンインストールしてから AVEVA Plant SCADA Access Anywhere 2023 以降をインストールすることで修正できます:
https://softwaresupportsp.aveva.com/#/producthub/details?id=ddbc4aa0-f607-4226-8625-08dabdf803e9

注: 古いバージョンのこれらの脆弱性に対するホット フィックスは利用できません。

謝辞

AVEVA からの感謝の意:

・CVE-2022-23854 の発見と責任ある開示に対する CRISEC の Jens Regel

・継続的な jQuery および OpenSSL ライブラリのメンテナンスのためのオープンソース コミュニティ

・アドバイザリの調整のための 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 SP800-82r2 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

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。