SECURITY BULLETIN AVEVA-2025-006

タイトル

AVEVA Edge（旧 InduSoft Web Studio）：危険なハッシュアルゴリズムの使用

評価

高（High）

発行者

AVEVA Product 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、以下の製品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リリースします。

- AVEVA Edge（旧 InduSoft Web Studio）2023 R2 およびそれ以前のすべてのバージョン。

脆弱性の技術的詳細

1. MD5 でハッシュ化されたパスワード

   この脆弱性が悪用された場合、Edge プロジェクトファイルまたは Edge オフラインキャッシュファイルへの読み取りアクセス権を持つ悪意のある攻撃者は、脆弱なハッシュ値に対する総当たり攻撃によって、Edge ユーザーのアプリネイティブパスワードまたは Active Directory パスワードをリバースエンジニアリングできる可能性があります。

   CWE-327：不完全または危険な暗号アルゴリズムの使用

   CVSSv4.0：8.3 高 | AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:N

   CVSSv3.1：8.4 高 | AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N

   CVE-2025-9317

推奨事項

AVEVA は、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、これらの脆弱性の影響を評価することを推奨します。影響を受ける製品バージョンおよび影響を受ける AVEVA Edge プロジェクトファイルを使用しているお客様は、悪用リスクを軽減するために、以下の対策を講じる必要があります。

- AVEVA Edge 2023 R2 P01 セキュリティアップデートを適用し、古いプロジェクトファイルを移行してください。
- 移行できないプロジェクト（バックアップや一時的なコピーなど）については、これらのファイルからのパスワード漏洩のリスクを評価し、これらの安全でないファイルを保護するために、より厳格な読み取りアクセス制御を実装してください。
- AVEVA Edge ユーザーにパスワードの変更を要求する

重要：パスワードハッシュアルゴリズムの変更に伴い、Edge プロジェクトの旧バージョンから 2023 R2 P01 への移行は一方通行となります。

セキュリティ更新ダウンロード

- AVEVA Edge 2023 R2 P01 以降では、この脆弱性に対処しています。
  AVEVA Edge 2023 R2 P01

防御策と一般的な考慮事項

以下の一般的な防御策を推奨します。

- 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読み込むすべてのフォルダ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、バックアップ、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。
- 強力なマスターパスワードを使用して、プロジェクトレベルでデータ保護を適用してください。設定手順については、AVEVA Edge「テクニカルリファレンスマニュアル」>「プロジェクト概要」>「追加プロジェクト設定の構成」>「オプション」タブ>「データ保護」を参照してください。
- プロジェクトドキュメント（スクリプトやワークシートなど）内で関数パラメータとしてパスワードが使用されている場合は、これらのパスワードを削除し、代わりにプロジェクトタグを使用することをお勧めします。タグの詳細については、AVEVA Edge「テクニカルリファレンスマニュアル」>「タグとタグデータベース」>「タグとプロジェクトデータベースについて」を参照してください。

謝辞

AVEVA は、以下の皆様に感謝の意を表します。

- João Varelas 氏：本脆弱性の発見、AVEVA 社との連携による情報開示、および AVEVA 社のセキュリティアップデートにおける修正テストの実施。
- CISA：アドバイザリの調整および CVE 番号の発行。

サポート

製品に関する AVEVA サポートへのお問い合わせ方法については、こちらのリンク（AVEVA カスタマーサポート）をご覧ください。
https://www.aveva.com/en/support-and-success/support-contact/
このセキュリティ通知に誤りや漏れを発見した場合は、サポートまでご報告ください。

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、AVEVA Security Central にアクセスしてください。https://softwaresupportsp.aveva.com/#/securitycentral

米国商務省産業制御システムセキュリティガイド

産業制御システムのセキュリティ確保に関する一般的な情報については、NIST の運用技術（OT）セキュリティガイドを参照してください。NIST SP800-82r3

NVD 共通脆弱性評価システム（CVSS v4.0）

米国国土安全保障省は、IT 脆弱性の特性と影響を伝えるためのオープンなフレームワークを提供する共通脆弱性評価システム（CVSS v4.0）を採用しました。CVSS v4.0 は、脆弱性の深刻度を反映した数値スコアと、そのスコアをテキストで表現した情報を生成します。スコアは 0.0（影響なし）から最大 10.0（最小限の労力で悪用可能な重大な影響）までの範囲です。詳細については、CVSS v4.0 の仕様書を参照してください。https://www.first.org/cvss/v4.0/specification-document

関係当局との連携

組織は、悪意のある活動が疑われる場合、定められた内部手順に従い、調査結果を関係当局に報告して、他の事例との追跡および関連付けを行うべきである。

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、明示的か黙示的かを問わず、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（ただしこれらに限定されない）一切の保証を否認します。AVEVA、その販売店、代理店、エージェント、従業員が提供する口頭または書面による情報や助言は、いかなる保証も構成するものではなく、お客様はそのような情報や助言に依拠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。

いかなる場合においても、AVEVA またはそのサプライヤー、ディーラー、販売代理店、エージェント、従業員は、契約または不法行為に基づく訴訟であるか否かを問わず、顧客または第三者が被った間接的、偶発的、特別、懲罰的、または結果的な損害、あるいは利益、収益、データ、または使用の損失に対する損害について、AVEVA がそのような損害の可能性について知らされていた場合であっても、一切責任を負いません。本契約に基づく、または本契約に関連する損害賠償および費用に対する AVEVA の責任（契約違反、不法行為、その他を問わず）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。