SECURITY BULLETIN AVEVA-2025-005

タイトル

AVEVA Application Server IDE：持続的なクロスサイトスクリプティングの脆弱性

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、AVEVA Application Server の統合開発環境（IDE）コンポーネントにおけ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。

Application Server は、AVEVA System Platform メディアの一部として配布されています。影響を受けるバージョンは以下のとおりです。

- Application Server 2023 R2 SP1 P02 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. App Objects ヘルプファイルにおける永続的なクロスサイトスクリプティングの脆弱性

   この脆弱性が悪用された場合、認証済みの悪意のあるユーザー（「aaConfigTools」権限を持つユーザー）は、App Objects のヘルプファイルを改ざんし、クロスサイトスクリプティング（XSS）インジェクションを永続的に実行できます。

   被害者ユーザーがこのインジェクションを実行すると、水平方向または垂直方向の権限昇格が発生する可能性があります。

   CWE-80: Web ページにおけるスクリプト関連 HTML タグの不適切な無効化

   CVSSv4.0: 7.2 高 | AV:L/AC:L/AT:N/PR:H/UI:P/VC:H/VI:L/VA:L/SC:H/SI:H/SA:H

   CVSSv3.1: 6.9 中 | AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:L/A:L

   CVE-2025-8386

推奨事項

AVEVA は、各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を使用しているお客様は、悪用されるリスクを軽減するためにセキュリティアップデートを適用してください。

セキュリティ更新

- 影響を受けるすべてのバージョンのアプリケーションサーバーIDE は、AVEVA System Platform 2023 R2 SP1 P03 以降にアップグレードすることで修正できます。
  System Platform 2023 R2 SP1 P03

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。

- 割り当てられたアクセス許可を監査し、「aaConfigTools」OS グループに信頼できるユーザーのみが追加されていることを確認してください。アプリケーションサーバーの OS セキュリティグループとアカウントに関する詳細については、以下の URL を参照してください。
  https://docs.aveva.com/bundle/sp-install/page/738031.html

謝辞

AVEVA は、以下の皆様に感謝の意を表します。

- CISA による勧告の調整および CVE の生成

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。