SECURITY BULLETIN AVEVA-2024-006

タイトル

AVEVA Reports for Operation：複数の脆弱性

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、上流のソフトウェアベンダーから提供された脆弱性に対する修正を含むセキュリティアップデートをリリースします。AVEVA Reports for Operations 2023 およびそれ以前のすべてのバージョンが、これらの脆弱性の影響を受けます。

脆弱性の技術的詳細

1. パス・トラバーサルによる任意コード実行

   この脆弱性が悪用されると、標準権限を持つローカル OS 認証ユーザーが、これらの製品がインストールされているマシン上のシステム権限に昇格され、ターゲットマシンが完全に侵害される可能性があります。

   CWE-22：制限付きディレクトリへのパス名の不適切な制限（パス・トラバーサル）

   CVSSv4.0：8.5 高 | AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

   CVSSv3.1：7.8 高 | AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

   CVE-2024-6618

2. 重要なファイルを上書きする

   この脆弱性が悪用されると、悪意のある攻撃者が AVEVA Reports for Operations プロジェクトの読み取りと書き込み、および/またはインストールファイルの改ざんを行う可能性があります。

   CWE-732: 重要なリソースに対する不適切なアクセス許可の割り当て

CVSSv4.0: 8.5 (高) | AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVSSv3.1: 7.8 (高) | AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2024-6619

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、セキュリティアップデートをできるだけ早く適用してください。

セキュリティ更新ダウンロード

影響を受けるすべてのバージョンは、AVEVA Reports for Operations 2023 R2 以降にアップグレードすることで修正できます。

AVEVA Reports for Operations 2023 R2

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。

- AVEVA Reports for Operations のインストールファイルおよびプロジェクトファイルのファイルとフォルダのアクセス制御リストを監査し、アクセスが意図したユーザーのみに制限されていることを確認します。

- AVEVA Reports for Operations のユーザーが、共有されたプロジェクトのソースが信頼できるものであることを、開いて実行する前に確認する手順を確立します。

謝辞

AVEVA は、以下の皆様に感謝の意を表します。

- この脆弱性の発見と責任ある開示にご協力いただいた Claroty の Team82
- 上流ベンダーである Ocean Data Systems
- 勧告の調整と CVE 番号の発行にご協力いただいた 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

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（米国国立標準技術研究所）の「運用技術（OT）セキュリティガイド」（NIST SP800-82r3）を参照してください。
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

NVD 共通脆弱性スコアリング 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達す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）を採用しています。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提供します。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

悪意のある活動が疑われる場合、組織は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、他の事例との関連性や追跡調査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。

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。