SECURITY BULLETIN AVEVA-2024-007

タイトル

AVEVA Reports for Operation：サービス拒否攻撃の脆弱性

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、SuiteLink Server の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。影響を受けるのは、以下の製品バージョンと配布メディアの組み合わせで SuiteLink Server がインストールされているノードのみです。

- SuiteLink 3.7.0 およびそれ以前のすべてのバージョン（スタンドアロン版）
- AVEVA Historian 2023 R2 P01 およびそれ以前のすべてのバージョン（AVEVA System Platform メディアで配布）
- AVEVA InTouch 2023 R2 P01 およびそれ以前のすべてのバージョン（AVEVA System Platform メディアで配布）
- Application Server 2023 R2 P01 およびそれ以前のすべてのバージョン（AVEVA System Platform メディアで配布）
- AVEVA Communication Drivers Pack 2023 R2 およびそれ以前のすべてのバージョン（スタンドアロン版または AVEVA System Platform メディアで配布）
- Batch Management 2023 およびそれ以前のすべてのバージョン

ノードに SuiteLink Server がインストールされているかどうかを確認するには、¥Program Files(x86)¥Common Files¥ArchestrA フォルダに「wwsls.dll」ファイルが存在するかどうかを確認してください。

SuiteLink クライアントはこの脆弱性の影響を受けないため、パッチを適用する必要はありません。

脆弱性の技術的詳細

1. サービス拒否（ボリューム型）

この脆弱性が悪用されると、SuiteLink サーバーが過剰なシステムリソースを消費し、攻撃期間中、データ I/O 処理が遅くなる可能性があります。

CWE-770：制限またはスロットリングなしのリソース割り当て

CVSSv4.0：8.7 高 | AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CVSSv3.1：7.5 高 | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2024-7113

推奨事項

AVEVA は、各組織が自社の運用環境、アーキテクチャ、および製品の実装状況に基づいて、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、できるだけ早くセキュリティアップデートを適用してください。

セキュリティ更新ダウンロード

（推奨）影響を受けるすべての製品およびバージョンは、SuiteLink 3.7.100 をインストールすることで修正できます。

SuiteLink 3.7.100

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。

- SuiteLink サーバーが信頼できる送信元からのトラフィックのみを受け入れるように、ホストファイアウォールおよび/またはネットワークファイアウォールルールを適用してください。デフォルトでは、SuiteLink はポート 5413 でリッスンします。

謝辞

AVEVA は、以下の機関に感謝の意を表します。

- 米国エネルギー省 CESER の CyTRICS プログラムの一環として、この脆弱性の発見と責任ある開示を行ったアイダホ国立研究所
- 勧告の調整と CVE の生成を行った CISA

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、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

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。