

# SECURITY BULLETIN AVEVA-2021-008

## タイトル

PCS ポータル アプリケーションの制御されていない検索パス要素による DLL 乗っ取り

## 評価

高 (High)

## 発行者

AVEVA Software Security Response Center

## 概要

AVEVA ソフトウェア LLC (“AVEVA”) は、プラットフォーム コモン サービス (PCS) ポータル バージョン 4.5.2、4.5.1、4.5.0、および 4.4.6 の DLL 乗っ取りの脆弱性に対処するためのセキュリティ更新プログラムを作成しました。この脆弱性が悪用されると、PCS ポータル アプリケーションのコンテキスト内で悪意のあるコードが実行される可能性があります。

次の製品は脆弱なバージョンの PCS ポータル アプリケーションを出荷しており、影響を受けます。:

- AVEVA™ System Platform 2020 R2 P01, 2020 R2, 2020
- AVEVA™ Work Tasks 2020 Update 1
- AVEVA™ Work Tasks 2020
- AVEVA™ Mobile Operator 2020
- AVEVA™ Manufacturing Execution System 2020
- AVEVA™ Batch Management 2020
- AVEVA™ Enterprise Data Management 2021

## 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。

影響を受けるバージョンの製品を使用しているお客様は、対応するセキュリティ更新プログラムをできるだけ早く適用する必要があります。

バージョン	セキュリティ アップデート	ダウンロードリンク
AVEVA™ Mobile Operator 2020 AVEVA™ Enterprise Data Management 2021 AVEVA™ System Platform 2020 R2 P01 AVEVA™ System Platform 2020 R2 AVEVA™ Work Tasks 2020 Update 1	PCS 4.5.3	<a href="#">(URL)</a>
AVEVA™ System Platform 2020 AVEVA™ Work Tasks 2020 AVEVA™ Manufacturing Execution System 2020 AVEVA™ Batch Management 2020	PCS 4.4.7	<a href="#">(URL)</a>

## 脆弱性の特徴付けと CVSSv3 評価

CWE-427: 制御されていない検索パス要素による DLL 乗っ取り

PCS Portal: 7.3 | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

## 謝辞

AVEVA からの感謝の意:

- ・この脆弱性の発見と責任ある開示について、Claroty の Noam Moshe に感謝します。
- ・アドバイザリの調整のための ICS-Cert

## 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>

## 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。