

SECURITY BULLETIN AVEVA-2023-003

タイトル

AVEVA™ Operations Control logger:ローカル権限昇格と任意のファイル削除の脆弱性

評価

高 (High)

発行者

AVEVA Software Security Response Center

概要

AVEVA Group Limited は、自社およびその子会社（「AVEVA」）を代表して、次のセキュリティアップデートを作成しました。AVEVA Operations Control Logger（旧名称 ArchestrA Logger）の脆弱性に対処します。次の製品に影響します。

- AVEVA System Platform 2020 R2 SP1 P01 およびそれ以前の全てのバージョン
- AVEVA Historian 2020 R2 SP1 P01 およびそれ以前の全てのバージョン
- AVEVA Application Server 2020 R2 SP1 P01 およびそれ以前の全てのバージョン
- AVEVA InTouch 2020 R2 SP1 P01 およびそれ以前の全てのバージョン
- AVEVA Enterprise Licensing 3.7.002 およびそれ以前の全てのバージョン(旧名称 License Manager)
- AVEVA Manufacturing Execution System 2020 P01 およびそれ以前の全てのバージョン（旧名称 Wonderware MES)
- AVEVA Recipe Management 2020 Update 1 Patch 2 およびそれ以前の全てのバージョン
- AVEVA Batch Management 2020 SP1 およびそれ以前の全てのバージョン
- AVEVA Edge 2020 R2 SP1 P01 およびそれ以前の全てのバージョン（旧名称 Indusoft Web Studio)
- AVEVA Work Tasks 2020 U2 およびそれ以前の全てのバージョン（旧名称 Workflow Management)
- AVEVA Plant SCADA 2020 R2 Update 15 およびそれ以前の全てのバージョン(旧名称 Citect)
- AVEVA Mobile Operator 2020 R1 およびそれ以前の全てのバージョン(旧名称 IntelaTrac Mobile Operator Rounds)
- AVEVA Communication Drivers Pack 2020 R2 SP1 およびそれ以前の全てのバージョン
- AVEVA Telemetry Server 2020 R2 SP1 およびそれ以前の全てのバージョン

脆弱性の技術的詳細

1. ローカル権限の昇格

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-250: [Execution with Unnecessary Privileges](#)

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

CVE-2023-33873

2. ローカルの任意ファイル削除

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でシステム権限を持つファイルを削除でき、サービス拒否が発生する可能性があります。

CWE-73: [External Control of File Name or Path](#)

CVSS v3.1: 5.5 Med | AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVE-2023-34982

推奨事項

AVEVA は、組織が運用環境、アーキテクチャ、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。影響を受ける製品を使用しているお客様は、出来るだけ早くセキュリティアップデートを適用する必要があります。

セキュリティ更新プログラムの適用に加えて、次の一般的な予防措置を講じる必要があります。

- ・ Guest または匿名のローカル OS アカウントが無効になっていることを確認します。
- ・ 信頼されたユーザーのみが、Operations Control Logger が実行されているノードにログインできるようにします。

セキュリティ更新プログラム

既知の互換性の問題

AVEVA System Platform 2020 ~ 2020 R2 SP1 は、以前に Operation Control Logger v22.1 のパッチが適用されている他の AVEVA 製品の上に新たにインストールすることはできません。詳細については、[Alart 000038736](#) を参照して下さい。

AVEVA System Platform, Historian, Application Server, and InTouch 2020 ～ 2020 R2 SP1 P01

- ・推奨する修正: AVEVA System Platform 2023 もしくはそれ以降へ更新する。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=64d4e12b-c363-4f35-8e8e-08da716924f7>

- ・代替の修正: AVEVA Operations Control Logger v22.1 以降をインストールします。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

AVEVA System Platform, Historian, Application Server, and InTouch 2017 U3 SP1 以前

- ・推奨する修正: AVEVA System Platform 2023 もしくはそれ以降へ更新する。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=64d4e12b-c363-4f35-8e8e-08da716924f7>

- ・代替の修正: まず、AVEVA System Platform 2020 R2 SP1 にアップグレードし、その後、AVEVA Operations Control Logger v22.1 以降をインストールします。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=c24f66e0-7e8f-4abb-0655-08d98ee90456>

<https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

AVEVA Enterprise Licensing 3.7.002 と、全てのそれ以前のバージョン

- ・推奨する修正: AVEVA Enterprise Licensing 4.0 もしくはそれ以降へ更新する。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=23f2f464-b581-4890-9b7e-079d38f9a7dd>

- ・代替の修正: AVEVA Operations Control Logger v22.1 もしくはそれ以降へ更新する。既知の互換性の問題を確認してください。

<https://softwaresupportsp.aveva.com/SiteAssets/GCSBerlin/index.aspx#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

AVEVA Manufacturing Execution System(MES) 2020 P02 と、全てのそれ以前のバージョン

- ・推奨する修正: AVEVA MES 2023 もしくはそれ以降へ更新する。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=50f245ed-210d-4047-8153-08daf99ef086>

- ・代替の修正: AVEVA Operations Control Logger v22.1 もしくはそれ以降へ更新する。既知の互換性の問題を確認してください。

<https://softwaresupportsp.aveva.com/SiteAssets/GCSBerlin/index.aspx#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

AVEVA Recipe Management 2020 Update 1 Patch 2 と、全てのそれ以前のバージョン

- ・推奨する修正: AVEVA Recipe Management 2023 もしくはそれ以降へ更新する。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=6e32c383-6be1-43d6-2a52-08db0eab7760>

- ・代替の修正: AVEVA Operations Control Logger v22.1 もしくはそれ以降へ更新する。既知の互換性の問題を確認してください。

<https://softwaresupportsp.aveva.com/SiteAssets/GCSBerlin/index.aspx#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

AVEVA Batch Management 2020 SP1 と、全てのそれ以前のバージョン

- ・推奨する修正: AVEVA Batch Management 2023 もしくはそれ以降へ更新する。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=b7fff900-39af-4d54-b8e7-210fd2d96a57>

- ・代替の修正: AVEVA Operations Control Logger v22.1 もしくはそれ以降へ更新する。既知の互換性の問題を確認してください。

<https://softwaresupportsp.aveva.com/SiteAssets/GCSBerlin/index.aspx#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

AVEVA Edge 2020 R2 SP1 P01 と、全てのそれ以前のバージョン（以前は Indusoft Web Studio とし

て知られていました。）

- ・推奨する修正: AVEVA Edge 2023 もしくはそれ以降へ更新する。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=0c8abaf3-2e4c-4be1-aa78-3ad445c58a16>

- ・代替の修正(1): AVEVA Edge 2020 R2 SP2 もしくはそれ以降へ更新する。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=bd805851-0c68-4343-15ee-08da9a4aa617>

- ・代替の修正(2): AVEVA Operations Control Logger v22.1 もしくはそれ以降へ更新する。既知の互換性の問題を確認してください。

<https://softwaresupportsp.aveva.com/SiteAssets/GCSBerlin/index.aspx#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

AVEVA Work Tasks 2020 U2 と、全てのそれ以前のバージョン（以前は Workflow Management として知られていました。）

- ・推奨する修正: AVEVA Work Tasks 2023 SP1 もしくはそれ以降へ更新する。もしも AVEVA Work Tasks を System Platform と同時に使用する場合、両方の製品を互換性のあるバージョンに更新する必要があります。[Technology Matrix](#) を確認してください。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=74b0e8a6-80c2-4884-a689-08daefd8f20e>

- ・代替の修正: AVEVA Operations Control Logger v22.1 もしくはそれ以降へ更新する。既知の互換性の問題を確認してください。

<https://softwaresupportsp.aveva.com/SiteAssets/GCSBerlin/index.aspx#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

AVEVA Plant SCADA 2020 R2 Update 15(2023/5)と、全てのそれ以前のバージョン（以前は Citect として知られていました。）

- ・推奨する修正: AVEVA Plant SCADA 2023 もしくはそれ以降へ更新する。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=892087d6-af69-439f-70f1-08da91049ae3>

- ・代替の修正(1): AVEVA Plant SCADA 2020 R2 Update 16(2023/6) もしくはそれ以降へ更新する。

<https://softwaresupportsp.aveva.com/#/producthub/details?id=78809d30-3f97-45c3-8d71-f537909aa3b5>

- ・代替の修正(2): AVEVA Operations Control Logger v22.1 もしくはそれ以降へ更新する。既知の互換性の問題を確認してください。

<https://softwaresupportsp.aveva.com/SiteAssets/GCSBerlin/index.aspx#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

AVEVA Mobile Operator 2020 R1 と、全てのそれ以前のバージョン（以前は IntelaTrac Mobile Operator として知られていました。）

- ・推奨する修正: AVEVA Mobile Operator 2020 R2 もしくはそれ以降へ更新する。
<https://softwaresupportsp.aveva.com/#/producthub/details?id=da960462-b522-4031-f287-08db1b42b39a>
- ・代替の修正(1): Mobile Operator 2020 ～ 2020 R1 の場合、AVEVA Operations Control Logger v22.1 もしくはそれ以降へ更新する。既知の互換性の問題を確認してください。
<https://softwaresupportsp.aveva.com/SiteAssets/GCSBerlin/index.aspx#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>
- ・代替の修正(2): IntelaTrac Mobile Operator 2017 SP2 もしくはそれ以前の場合、最初に AVEVA Mobile Operator 2020 に更新し、その後に AVEVA Operations Control Logger v22.1 もしくはそれ以降へ更新する。既知の互換性の問題を確認してください。
<https://softwaresupportsp.aveva.com/#/producthub/details?id=37a51ba1-4a40-4c69-44cd-08d8fd519f4f>
<https://softwaresupportsp.aveva.com/SiteAssets/GCSBerlin/index.aspx#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

AVEVA Communication Drivers Pack 2020 R2 SP1 と、全てのそれ以前のバージョン

- ・推奨する修正: AVEVA Communication Drivers Pack 2023.1 もしくはそれ以降へ更新する。
<https://softwaresupportsp.aveva.com/#/producthub/details?id=e1af0884-b3c6-4d0f-a6b6-47507b398690>
- ・代替の修正: AVEVA Operations Control Logger v22.1 もしくはそれ以降へ更新する。既知の互換性の問題を確認してください。
<https://softwaresupportsp.aveva.com/SiteAssets/GCSBerlin/index.aspx#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

AVEVA Telemetry Server 2020 R2 SP1 と、全てのそれ以前のバージョン

- ・推奨する修正: AVEVA Telemetry Server 2020 R2 SP2 もしくはそれ以降へ更新する。
<https://softwaresupportsp.aveva.com/#/producthub/details?id=e1af0884-b3c6-4d0f-a6b6-47507b398690>
- ・代替の修正: AVEVA Operations Control Logger v22.1 もしくはそれ以降へ更新する。既知の互換性の問題を確認してください。

<https://softwaresupportsp.aveva.com/SiteAssets/GCSBerlin/index.aspx#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8>

謝辞

AVEVA からの感謝の意:

- ・ Equinor の Lukasz Piotrowski 氏、発見、責任ある開示、修正のテストに協力
- ・ CISA による勧告の調整

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>

当局との調整

疑わしい悪意のある活動を観察している組織は、確立された内部手順に従い、調査結果を該当する当局に報告して、追跡と他のインシデントとの関連付け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。

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。