SECURITY BULLETIN AVEVA-2021-002

タイトル

System Platform – 任意のコード実行またはサービス拒否への AutoBuild チェーンの脆弱性

評価

高（High）

発行者

AVEVA Software Security Response Center

概要

AVEVA ソフトウェア LLC (“AVEVA”) は、AutoBuild 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。 脆弱な AutoBuild コンポーネントは、AVEVA™ System Platform バージョン 2017 から 2020 R2 P01 (包括的) に存在します。 これらの脆弱性を悪用して連鎖させると、悪意のあるエンティティがシステム権限で任意のコードを実行したり、サービス拒否を引き起こしたりする可能性があります。

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。

AutoBuild サービスは、構成時にシステム プラットフォームの GR ノードでのみ使用することを目的としています。 Windows サービス アプレットを使用して、すべてのランタイム ノードで無効にする必要があります。
さらに、AutoBuild 機能が GR ノードで使用されていない場合は、アタッチを必要としない代替緩和策として、GR ノードで AutoBuild サービスを無効にすることもできます。

AutoBuild 機能を継続的に使用する必要があり、システム プラットフォーム バージョン 2017 から 2020 R2 P01 (包括的) で無効にできないお客様は、脆弱性の影響を受けます。まず、以下にリストされているシステム プラットフォーム バージョンのいずれかにアップグレードしてから、対応するセキュリテ

ィ更新プログラムを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
System Platform 2020 R2 P01 2020 R2 2020	AVEVA™ Communication Drivers Pack 2020 R2.1 を適用	(URL)
System Platform 2017 U3 SP1 P01	最初に、AVEVA™ Communication Drivers Pack 2020 R2* を適用。 次に、AVEVA™ Communication Drivers Pack 2020 R2.1 を適用。	(URL) (URL)

*注意: System Platform 2017 U3 SP1 P01 の上に AVEVA™ Communication Drivers Pack 2020 R2 を適用するには、ライセンス認証が必要です。 ライセンスの互換性については、サポートにお問い合わせください。

脆弱性の特徴付けと CVSSv3 評価

CWE-22: パス トラバーサル

CWE-306: 重要な機能の認証がありません

CWE-346: オリジン検証エラー

CWE-347: デジタル署名の不適切な検証

AutoBuild コード実行脆弱性チェーン: 8.8 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE-248: キャッチされない例外

AutoBuild サービス拒否: 6.5 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

謝辞

AVEVA からの感謝の意:

・Claroty の Sharon Brizinov 氏は、脆弱性の発見、責任ある開示、および AVEVA の修正の検証について

・アドバイザリと CVE 作成の調整のための 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。