SECURITY BULLETIN AVEVA-2021-003

タイトル

SuiteLink サーバー – 複数のサービス拒否 (DoS) 脆弱性と理論上のリモート コード実行 (RCE)

評価

高（High）

発行者

AVEVA Software Security Response Center

概要

AVEVA ソフトウェア LLC (“AVEVA”) は、SuiteLink Server の脆弱性に対処するためのセキュリティ アップデートを作成しました。 この脆弱性が悪用されると、悪意のあるパケットの解析中に SuiteLink Server がクラッシュします。 さらに、リモートでコードを実行することは理論的には可能かもしれませんが、概念実証は存在しません。 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。

以下の製品には脆弱なバージョンの SuiteLink Server が含まれており、影響を受けます。:

・AVEVA™ System Platform 2020 R2 P01 およびそれ以前のすべてのバージョン
・AVEVA™ InTouch 2020 R2 P01 およびそれ以前のすべてのバージョン
・AVEVA™ Historian 2020 R2 P01 およびそれ以前のすべてのバージョン
・AVEVA™ Communication Drivers Pack 2020 R2 およびそれ以前のすべてのバージョン
・AVEVA™ Operations Integration Core 3.0 およびそれ以前のすべてのバージョン
・AVEVA™ Data Acquisition Servers のすべてのバージョン
・AVEVA™ Batch Management 2020 およびそれ以前のすべてのバージョン
・AVEVA™ MES 2014 R2 およびそれ以前のすべてのバージョン

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適用する必要があります。 更新プログラムのサブセットには、アクティベーション ベースのライセンスが必要であることに注意してください。

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™ InTouch 2014 R2 SP1 P02 ～ 2020 R2 P01 (包括的)	AVEVA™ SuiteLink 3.2.002	(URL)
AVEVA™ Historian 2014 R2 SP1 P02 ～ 2020 R2 P01 (包括的)	AVEVA™ SuiteLink 3.2.002	(URL)
AVEVA™ Communication Drivers Pack 2020 R2 と、それ以前	AVEVA™ SuiteLink 3.2.002 もしくは、 AVEVA™ Communication Drivers Pack 2020 R2.1 (注: アクティベーションベースのライセンスが必要です。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)	(URL) (URL)
AVEVA™ Operations Integration Core 3.0 と、それ以前		
すべての Data Acquisition Server のすべての成熟したバージョン		
AVEVA™ Batch Management 2020	AVEVA™ SuiteLink 3.2.002	(URL)
AVEVA™ Batch Management 2017 U1 と、それ以前	最初に AVEVA™ Batch Management 2020 へのアップグレードを行い、次に AVEVA™ SuiteLink 3.2.002 を適用してください。	(URL) (URL)
AVEVA™ MES 2014 R2 と、それ以前	AVEVA™ MES 2014 R3 以降にアップグレード	(URL)

脆弱性の特徴付けと CVSSv3 評価

CWE-122: ヒープベースのバッファ オーバーフロー

SuiteLink サーバー (理論上の RCE): 8.1 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

SuiteLink サーバー DoS: 7.5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE-476: Null ポインター逆参照

SuiteLink サーバー DoS: 7.5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE-755: 例外条件の不適切な処理:

SuiteLink サーバー DoS: 7.5 | CVSS:3.1/AV:N/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 Common Vulnerability and Exposure (CVE) の作成を調整するための 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。