ICS 脆弱性分析レポート — 2022 年度下期 —

一般社団法人 JPCERT コーディネーションセンター

2023 年 6 月 29 日

JPCERT CC®

目次

1. はじめに 3
1.1. 本文書の目的 3
1.2. 2022 年度下期に注目した脆弱性情報 3
2. ICS 関連製品固有の通信プロトコルに関連する ICS 関連の攻撃手法および対策 3
2.1. T0819：Exploit Public-Facing Application に対するリスク軽減策 6
2.2. T0883：Internet Accessible Device に対するリスク軽減策 6
2.3. T0886：Remote Service に対するリスク軽減策 6
2.4. T0871：Execution through API に対するリスク軽減策 7
2.5. T0866：Exploitation of Remote Service に対するリスク軽減策 8
2.6. T0867：Lateral Tool Transfer に対するリスク軽減策 8
2.7. T0843：Program Download に対するリスク軽減策 9
2.8. T0802：Automated Collection に対するリスク軽減策 9
2.9. T0845：Program Upload に対するリスク軽減策 10
2.10. T0816：Device Restart/Shutdown に対するリスク軽減策 10
3. ICS 製品の脆弱性情報への対応のお願い 12
付録 A. 2022 年度下期に確認した ICS 関連製品の脆弱性情報 13

1. はじめに

1.1. 本文書の目的

本文書は、直近の半期間に公表された ICS 関連製品の脆弱性情報の中から特徴的なものをピックアップし、その内容や ICS 全体への影響などを解説したものです。本文書が、ICS ユーザー組織のセキュリティ担当者が ICS 関連製品の脆弱性の背景と意味合いを理解する上での一助となれば幸いです。

1.2. 2022 年度下期に注目した脆弱性情報

2022 年度下期（2022 年 10 月 1 日から 2023 年 3 月 31 日までの間）に公表された ICS 関連製品の脆弱性情報にも Web インタフェースの脆弱性に関するものが複数ありました。また、ICS 機器の設定および監視データの取得などに使用される独自の通信プロトコルの脆弱性（CVE-2022-0902、CVE-2023-0321）や特定ベンダー製ソフトウェアのライセンス認証に使用される独自の通信プロトコルの脆弱性（CVE-2022-43513、CVE-2022-43514）、データヒストリアンにデータを送信する際に使用される独自の通信プロトコルの脆弱性（CVE-2022-43663、CVE-2022-45124）など、ICS 固有の通信プロトコルに関連するものも複数あり、その一部について本レポートで紹介いたします。

ICS 固有の通信プロトコルの中には、クローズドなネットワーク環境での使用を前提としている、少ない計算資源で高速な処理を実現する必要がある、シリアル通信で使用されていたプロトコルをそのままの仕様で TCP/IP 化したなど、セキュリティ機能を実装する必要性の検討もないまま、セキュリティ機能が実装されていないプロトコルがあります。以前より、これらについては「設計に由来するセキュリティ問題」として度々の指摘がなされていますが、近年では、セキュリティ研究者がそれらを脆弱性と捉えて指摘するケース [1]が出てきています。また、誰しもがアクセスし自由に操作できるとみられる ICS 関連製品がインターネットに直結されている場合さえあります。そのため、利用機器を棚卸して、ICS 固有の通信プロトコルを使っているものの有無を調べ、該当するものがあった場合には、必要なアクセス制限を施すなど、脆弱性の有無に関わらず脆弱性を意識した運用が肝要です。本レポートでは、こうした脆弱性が招いているセキュリティリスクを理解する際の参考として、MITRE の ATT&CK for ICS[2] による評価を紹介します。

2. ICS 固有の通信プロトコルを悪用した ICS 関連の攻撃手法および対策

通信プロトコルを悪用した ICS への攻撃は ATT&CK for ICS（v13）の 12 段階のうち「初期アクセス」「実行」「ラテラルムーブメント（侵入拡大）」「収集」「応答機能の妨害」のフェーズで行われる可能性があるとされています。[表 1] に ICS 固有の通信プロトコルを悪用する攻撃に使用されると考えられる技術・手法（Techniques）と、それらの技術・手法が使用されるフェーズ（Tactics）をまとめました。

---

1 Forescount | OT:ICEFALL
https://www.forescout.com/research-labs/ot-icefall/

2 MITRE ATT&CK | ICS Teqhniques
https://attack.mitre.org/techniques/ics/

［表 1：ICS 固有の通信プロトコルを悪用する攻撃が記載された攻撃フェーズおよび技術・手法］

攻撃のフェーズ（Tactics）	攻撃に使用される技術・手法（Techniques）
TA0108：Initial Access 初期アクセス	T0819：Exploit Public-Facing Application 攻撃者が、産業用ネットワークへの初期アクセスを得るために、インターネット経由でアクセス可能なソフトウェアの欠陥を悪用する可能性がある。
	T0883：Internet Accessible Device 攻撃者が、適切な保護がされないまま意図せず、あるいは意図的にインターネットに直接接続されたシステムを経由して侵入する可能性がある。
	T0886：Remote Service 攻撃者が、資産やネットワークセグメント間を移動するためにリモートサービスを使用する可能性がある。
TA0104：Execution 実行	T0871：Execution through API 攻撃者が、ICS 機器と ICS 関連ソフトウェアとの間の通信に使用されるアプリケーションプログラムインタフェース（API）を使用する可能性がある。
TA0109：Lateral Movement ラテラルムーブメント（侵入拡大）	T0866：Exploitation of Remote Service 攻撃者が、プログラム、サービス、オペレーティングシステムやカーネル自体のプログラムエラーを使用するために、ソフトウェアの脆弱性を悪用し、リモートサービスを不正使用する可能性がある。
	T0867：Lateral Tool Transfer 攻撃者が、作戦の過程でツールや他のファイルを準備するため、あるシステムから別のシステムにそれらを転送する可能性がある。
	T0843：Program Download 攻撃者が、ユーザープログラムをコントローラーに転送するためにプログラムのダウンロードを実行する可能性がある。

攻撃のフェーズ（Tactics）	攻撃に使用される技術・手法（Techniques）
TA0109：Lateral Movement ラテラルムーブメント（侵入拡大）	T0886：Remote Service 攻撃者が、資産やネットワークセグメント間を移動するためにリモートサービスを使用する可能性がある。
TA0100：Collection 収集	T0802：Automated Collection 攻撃者が、ツールやスクリプトを使用して ICS 環境の情報収集を自動化する可能性がある。自動収集では、制御システム環境で利用可能なネイティブの制御プロトコルやツールが使用される可能性がある。
	T0845：Program Upload 攻撃者が、産業プロセスに関する情報を収集するために PLC からプログラムをアップロードする可能性がある。
TA0107：Inhabit Response Function 応答機能の妨害	T0816：Device Restart/Shutdown 攻撃者が、物理的なプロセスを混乱させるために ICS 環境のデバイスを強制的に再起動したり、シャットダウンしたりする可能性がある。これらの機能は標準機能としてデバイスに存在し、Web インタフェースや CLI、ネットワークプロトコルコマンドを使用して実行される。

［表 1］によれば、ICS 固有の通信プロトコルの脆弱性を悪用した攻撃は、初期侵入や侵入直後のコード等の実行、侵入後の横断的侵害、侵害したネットワーク内の情報収集、応答機能の妨害に使用される可能性があると考えられます。製品固有の通信プロトコルに関する脆弱性の悪用が侵入の起点になることは情報システム関連の製品でも同様ですが、ICS 固有のプロトコルでは、次のような脅威シナリオが特徴的です。

- ICS 機器と ICS 関連ソフトウェアとの間（例えばエンジニアリングソフトウェアによる機器設定など）の通信に使用される API 経由で任意のコードが実行される可能性がある（T0871）
- ユーザープログラムをコントローラーに転送するためにプログラムダウンロードを使用される可能性がある（T0843）
- ICS 環境の情報収集を自動化するために使用される可能性がある（T0802）
- 産業プロセスの情報を収集するために PLC からプログラムをアップロードする可能性がある（T0854）
- 物理的なプロセスを混乱させるために ICS 環境のデバイスを強制的に再起動したり、シャットダウンしたりする可能性がある（T0816）

また、「実行（TA0104）」のフェーズに記載されている悪意あるコードを実行する技術は、他の戦術の技術と組みあわせて使用されることもあり、ネットワークの「発見（TA0102）」と「収集（TA0100）」やオペレーションへの影響、応答機能の妨害を支援するとされています。これらの点を踏まえると、ICS 製品固有の通信プロトコルの脆弱性の悪用は ICS 環境の広い範囲にさまざまな影響を与える可能性があります。CVSS による脆弱性の深刻度は、脆弱性による直接の影響のみが評価されており、間接的に生じる影響までは考慮されていません。そのため、影響を受ける ICS 関連製品だけでなく、同製品が影響を受けた場合の広がりについても意識しておく必要があります。

ATT&CK for ICS では、ICS 固有の通信プロトコルを悪用する攻撃に関連する技術・手法に対するリスク軽減策もまとめられています。各技術・手法に対するリスク軽減策を 2.1～2.10 に記載いたしましたので、ICS ユーザー組織の担当者はこれらの対策の実施についてご検討ください。

2.1. T0819：Exploit Public-Facing Application に対するリスク軽減策

- ソフトウェア制限ポリシー、Windows の AppLocker、Linux の SELinux や AppArmor を使用して悪用されたターゲットがアクセス可能な他のプロセスやシステム機能を制限する（M0948）
- Web Application Firewall を使用してアプリケーションの公開を制限し、悪意あるトラフィックがアプリケーションに到達するのを防止する（M0950）
- 外部向けのサーバーやサービスは、DMZ や独立したホスティングインフラストラクチャを使用して他のネットワークから分離する（M0930）
- サービスアカウントに最小限の権限を使用する（M0926）
- 外部向けのシステムの脆弱性を定期的にスキャンする。また、スキャンや一般公開により重大な脆弱性が発見された場合に備え、迅速にパッチを適用する手順を確立する（M0951、M0916）

2.2. T0883：Internet Accessible Device に対するリスク軽減策

- ネットワークプロキシ、ゲートウェイ、ファイアウォールを使用し、内部システムへの直接のリモートアクセスを制限する。また、インターネットにアクセス可能なデバイスを定期的に棚卸し、想定と異なるかどうかを確認する（M0930）

2.3. T0886：Remote Service に対するリスク軽減策

- アクセス管理技術を使用して重要なリモートサービスの認証を強化する。例としては、デバイス管理サービス（telnet、SSH など）、データアクセスサーバー（HTTP、Historian など）、HMI セッション（RDP、VNC など）があるが、これらに限定されない（M0801）

- システムの操作を制御するための GUI セッションの制限に対応する権限を提供する（HMI の読み取り専用モードと読み取り/書き込みモードなど）。オペレーターやエンジニアなどのローカルユーザーが、リモートセッションよりも優先され、必要に応じてリモートセッションの制御を回復する権限を持っていることを確認する。リモートアクセスセッション（RDP、VNC など）が、ICS の制御（特に HMI）に使用されるローカルセッションを引き継ぐことを防止する（M0800）
- リモートサービスのアプリケーション層プロトコルメッセージをフィルタリングし、不正な活動をブロックする（M0937）
- すべてのリモートサービスで、ユーザーアクセスを提供する前に強力な認証を要求する（M0804）
- ホストベースのファイルやシステムホストファイルで実装可能なネットワーク許可リストを使用して、デバイスの外部接続（IP アドレス、MAC アドレス、ポート、プロトコル）を指定する（M0807）
- 単一方向の通信のみが許可されている DMZ を使用してビジネス環境と OT 環境間のソフトウェアの移動を分離し、制御する。OT 環境からの Web アクセスは制限する。一過性のサイバー資産（TCA）を含め、エンジニアリングワークステーションは、インターネットおよび電子メールを含む外部ネットワークの接続を最小限にする。また、これらのデバイスが複数のネットワークにデュアルホームされる範囲を制限する（M0930）
- パスワードの総当たりによる横断的侵害を防止するため、安全なパスワードの要求を強制する（M0927）
- リモートサービスへのすべての通信セッションを認証して不正アクセスを防止する（M0813）
- リモートサービスを利用できるアカウントを制限する。例えば、特定のプログラムしか実行できないように SSH を設定するなど、侵害されるリスクが高いアカウントの権限を制限する（M0918）

2.4. T0871：Execution through API に対するリスク軽減策

- ユーザーの識別や認証の機能がないフィールド機器に対し、アクセス管理技術を使用して認可ポリシーと認可決定を強制する。これらの技術には、認証されていないユーザーへのアクセスを防止すると同時にユーザーの資格情報を最初に検証する認証サービスと統合するため、インラインネットワークデバイスまたはゲートウェイシステムが使用される（M0801）
- 実行されているすべての API（特に、PLC などのコントローラー上でホストされる API）について、ユーザーアクセスに対する適切な認証を強制する。ユーザーのアクセスを必要最小限の API コールのみにする（M0800）
- コード実行を可能にする API コールの公開を最小限にする（M0938）
- リモートシステムまたはローカルプロセス上のすべての API について、コードまたはシステムの変更を実行する前にユーザー認証を要求する（M0804）

2.5. T0866：Exploitation of Remote Service に対するリスク軽減策

- サンドボックスを使用して未知またはパッチ未適用の脆弱性を悪用する攻撃者の活動を困難にする。その他の種類の仮想化やアプリケーションのマクロセグメンテーションを使用して、ある種の悪用による影響を軽減する。これらのシステムにおける更なる悪用や欠陥のリスクは依然として存在する可能性がある（M0948）
- 不要なポートやサービスを閉じ、発見されるリスクや悪用される可能性を防ぐ（M0942）
- Windows Defender Exploit Guard（WDEG）や Enhanced Mitigation Experience Toolkit（EMET）など、エクスプロイト時に使用される動作を検出するセキュリティアプリケーションを使用して一部のエクスプロイトの動作を緩和する。ソフトウェア悪用の発生を潜在的に特定し、阻止するために制御フローの整合性をチェックする。これらの保護機能の多くは、アーキテクチャやターゲットアプリケーションのバイナリの互換性に依存するため、ターゲットとなるすべてのソフトウェアやサービスに対して機能するとは限らない（M0950）
- ネットワークやシステムを適切に分離し、重要なシステムやサービスの通信へのアクセスを減少させる（M0930）
- サービスアカウントの権限とアクセスを最小限に抑え、悪用された場合の影響を抑止する（M0926）
- 堅牢なサイバー脅威インテリジェンスの能力を構築し、特定の組織に対して、どのような種類およびレベルの脅威がソフトウェアの悪用やゼロデイを使用する可能性があるかを判断できるようにする（M0919）
- 企業内のエンドポイントおよびサーバーのパッチマネージメントを導入し、ソフトウェアを定期的に更新する（M0951）
- 利用可能なサービスについて内部ネットワークを定期的にスキャンし、新しいサービスや潜在的に脆弱なサービスを特定する（M0916）

2.6. T0867：Lateral Tool Transfer に対するリスク軽減策

- ネットワーク侵入検知および防止システムのネットワークシグネチャを使用して、特定のマルウェアのトラフィックや、FTP などの既知のツールやプロトコルでの異常なデータ転送を識別し、ネットワークレベルでの活動を軽減する。シグネチャの多くは、プロトコルのユニークなインディケータに対応しており、個別の攻撃者およびツールによって使用される特定の難読化技術に基づいたり、さまざまなマルウェアファミリーやバージョンで異なったりする可能性がある。また攻撃者は、ツールで使用されている C2 サーバーのシグネチャを変更したり、一般的な防御ツールによる検出を回避したりするような方法でプロトコルを構築したりする可能性がある（M0931）

2.7. T0843：Program Download に対するリスク軽減策

- デバイスの状態、ロジック、プログラムへのアクセスや変更を許可する前に、フィールドコントローラーへのすべてのアクセスを認証する。Centralized Authentication の技術は、ICS 全体で必要とされる多数のフィールドコントローラーのアカウントを管理するのに役立つ（M0801）
- コントローラーにロードされた制御ロジックやプログラムの完全性を検証する機能を提供する。CRC やチェックサムなどの技術が一般的に使用されているが、これらは暗号強度が不十分で衝突に対して脆弱であるため、暗号化ハッシュ関数（SHA-2、SHA-3 など）の使用が望ましい（M0947）
- すべてのフィールドコントローラーについて、可能であればロールベースのアクセスメカニズムを実装し、プログラムの変更を特定のユーザー（例えば、エンジニア、フィールド技術者）のみに制限する（M0800）
- 安全または制御資産にインストールされたプログラムが変更されていないことを検証するためにコード署名を利用する（M0945）
- 無許可のシステム変更を防ぐため、デバイス管理に使用されるプロトコルのすべてのネットワークメッセージを認証する（M0802）
- 不正なデバイスの設定を防ぐため、プログラムのダウンロードに関連するプロトコルおよびペイロードをフィルタリングする（M0937）
- リモートまたはローカルのすべての管理セッションにおいて、すべてのフィールドコントローラーにユーザーに認証を要求する。また、アカウント使用ポリシー、パスワードポリシー、およびユーザーアカウント管理をサポートする認証メカニズムを使用する（M0804）
- ホストベースの許可リストを使用して、デバイスが許可されていないシステムからの接続を受け入れないようにする。例えば、許可リストを使用して、デバイスがマスターステーションまたは既知の管理用ワークステーション、エンジニアリングワークステーションとしか接続できないようにする（M0807）
- 運用ネットワークとシステムを分離し、重要なシステム機能へのアクセスを所定の管理システムに制限する（M0930）
- ソフトウェアやデバイスからの接続を認証し、不正なシステムから保護された管理機能へのアクセスを防止する（M0813）

2.8. T0802：Automated Collection に対するリスク軽減策

- ネットワーク許可リストを使用して、ネットワーク機器（通信サーバー、シリアル－イーサネット変換機など）やサービスへの不要な接続を制限する。特にデバイスがサポートする同時セッション数に制限がある場合は、その制限を設ける（M0807）
- 産業情報を含む制御サーバーやフィールドデバイス、特に一般的な制御プロトコル（DNP3、OPC など）に使用されるサービスに対する、不正なシステムからのアクセスを防止する（M0930）

2.9. T0845：Program Upload に対するリスク軽減策

- デバイスの状態、ロジック、プログラムへのアクセスや変更を許可する前に、フィールドコントローラーへのすべてのアクセスを認証する。Centralized Authentication の技術は、ICS 全体で必要とされる多数のフィールドコントローラーのアカウントを管理するのに役立つ（M0801）
- すべてのフィールドコントローラーについて、可能であればロールベースのアクセスメカニズムを実装し、プログラムのアップロードを特定のユーザー（例えば、エンジニア、フィールド技術者）のみに制限する（M0800）
- 無許可のシステム変更を防ぐため、デバイス管理に使用されるプロトコルのすべてのネットワークメッセージを認証する（M0802）
- 機器設定への不正アクセスを防ぐため、プログラムのアップロードに関連するプロトコルおよびペイロードをフィルタリングする（M0937）
- リモートまたはローカルのすべての管理セッションにおいて、すべてのフィールドコントローラーにユーザーに認証を要求する。また、アカウント使用ポリシー、パスワードポリシー、およびユーザーアカウント管理をサポートする認証メカニズムを使用する（M0804）
- ホストベースの許可リストを使用して、デバイスが許可されていないシステムからの接続を受け入れないようにする。例えば、許可リストを使用して、デバイスがマスターステーションまたは既知の管理用ワークステーション、エンジニアリングワークステーションとしか接続できないようにする（M0807）
- 運用ネットワークとシステムを分離し、重要なシステム機能へのアクセスを所定の管理システムに制限する（M0930）
- ソフトウェアやデバイスからの接続を認証し、不正なシステムから保護された管理機能へのアクセスを防止する（M0813）

2.10. T0816：Device Restart/Shutdown に対するリスク軽減策

- すべての管理機能が含まれているすべてのデバイスまたはシステムの変更には認証を要求する。特にデバイスに強力な認証や認可の機能が備わっていない場合は、すべての管理インタフェースへのアクセスに対して認可を強制するためにアクセス管理技術を使用する（M0801）
- すべてのフィールドコントローラーについて、可能であればロールベースのアクセスメカニズムを実装し、プログラムの変更を特定のユーザー（例えば、エンジニア、フィールド技術者）のみに制限する（M0800）
- 制御機能に使用されるプロトコルは、真正性を保つために MAC 機能またはデジタル署名を使用する。そうでない場合は、Bump In The Wire デバイスまたは VPN を使用して、これをサポートする能力がないデバイス（レガシーコントローラー、RTU など）間での通信の真正性を保持する（M0802）
- 必要がない場合、デバイスのシャットダウンを可能するリモートコマンドを無効にする。例えば、DNP3 の 0x0D ファンクションコードや不要なデバイス管理機能などがある（M0942）

- DNP3 の 0x0D ファンクションコードなどのデバイスのシャットダウンや再起動を始動するために使用される制御用プロトコルの機能や、デバイスのシャットダウンを引き起こすために使用可能な脆弱性（CVE-2014-9195、CVE-2015-5374 など）をブロックするためにアプリケーション拒否リストを使用する（M0937）
- リモートまたはローカルのすべての管理セッションにおいて、すべてのフィールドコントローラーにユーザーに認証を要求する。また、アカウント使用ポリシー、パスワードポリシー、およびユーザーアカウント管理をサポートする認証メカニズムを使用する（M0804）
- ホストベースの許可リストを使用して、デバイスが許可されていないシステムからの接続を受け入れないようにする。例えば、許可リストを使用して、デバイスがマスターステーションまたは既知の管理用ワークステーション、エンジニアリングワークステーションとしか接続できないようにする（M0807）
- 運用ネットワークとシステムを分離し、重要なシステム機能へのアクセスを所定の管理システムに制限する（M0930）
- ソフトウェアやデバイスからの接続を認証し、不正なシステムから保護された管理機能へのアクセスを防止する（M0813）

3. ICS 関連製品の脆弱性情報への対応のお願い

深刻な不具合であれば対応の優先度が高くなりますが、脆弱性の場合には、それを悪用した攻撃が行われるまで、その問題は顕在化しないので、対策が先延ばしになりがちです。脆弱性によって ICS が抱えるリスクを踏まえ、実施時期や効果的な対策の方法（例えば、アップデートではなく、対処策（ワークアラウンド）にて対策する）を検討してください。リスクの評価には、本文書で取り上げた方法だけでなく、システムの重要度や設置環境などの環境要因に基づく考え方もあります。例えば、ネットワーク経由でリモートから攻撃が可能な脆弱性の情報が公表されても、その製品がネットワークに接続されていないケースでは、脆弱性そのものを悪用する経路がありません。

JPCERT/CC では、ICS について注意喚起や脆弱性情報の提供を行っています。
詳細は、次の Web ページをご参照ください。

Japan Vulnerability Notes（JVN）
https://jvn.jp/

制御システムセキュリティ情報共有ポータルサイト ConPaS
https://www.jpcert.or.jp/ics/ics-community.html

なお、「付録 A. 2022 年度下期に確認した ICS 関連製品の脆弱性情報」に記載した脆弱性情報などについてご提供いただける情報がございましたら JPCERT/CC までご連絡ください。

一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
制御システムセキュリティ対策グループ
Email：icsr@jpcert.or.jp

付録 A. 2022 年度下期に確認した ICS 関連製品の脆弱性情報

2022 年度下期に JPCERT/CC が「注意喚起」の発行を検討するために確認を行った ICS 関連製品の脆弱性情報は、[表 2] のとおり 29 件でした。これらの脆弱性情報は、インターネットなどの公開情報から収集したものの中から「想定される影響」「CVSS v3 基本評価基準による評価結果」「PoC コードの公開状況」「製品の国内流通状況」「対策の提供状況」を踏まえた一次評価を行い、日本国内の ICS ユーザー組織に直ちに影響が出る恐れがあると判断したものです。これらの情報に対し、「影響を受ける製品の詳細情報（用途や使われ方、使用されている技術など）」「影響を受けるコンポーネントの範囲」「攻撃が行われた場合に想定される被害」などの技術的な観点から確認を行いました。

[表 2：2022 年度下期に JPCERT/CC が確認した ICS 関連製品の脆弱性情報一覧]

No.	情報確認日	タイトル	原因箇所
1	2022/10/13	WAGO 製 PLC 750 シリーズにおけるリソース枯渇の脆弱性	RTOS の脆弱性の継承
2	2022/10/19	Phoenix Contact 製 PLCnext における複数の脆弱性	ライブラリの脆弱性の継承
3	2022/11/16	Meinberg 製 LANTIME Firemware における複数の脆弱性	ライブラリの脆弱性の継承
4	2022/11/21	Delta Electronics 製 DIAEnergie における複数の脆弱性	Web インタフェースの脆弱性
5	2022/11/21	Siemens 製 APOGEE PXC、TALON TC における不適切な認証の脆弱性	Web インタフェースの脆弱性
6	2022/11/22	AVEVA 製 InTouch Access Anywhere Secure Gateway におけるパストラバーサルの脆弱性	Web インタフェースの脆弱性
7	2022/11/22	Belden および Hirschmann 製ソフトウェア製品における複数の脆弱性	ライブラリの脆弱性の継承
8	2022/11/22	ABB 製 Flow Computer および Remote Controller におけるパストラバーサルの脆弱性	ネットワーク処理関連の脆弱性
9	2022/11/29	Pilz 製 PAS4000 における複数の脆弱性	ライブラリの脆弱性の継承
10	2022/11/29	Pilz 製 PASvisu および PMI における複数の脆弱性	ライブラリの脆弱性の継承
11	2022/11/29	Hirschmann 製 BAT-C2 における複数の脆弱性	Web インタフェースの脆弱性
12	2022/11/29	Hirschmann 製 HiLCOS 関連製品における無限ループの脆弱性	ライブラリの脆弱性の継承
13	2022/12/6	複数の Festo 製品における複数の脆弱性	ライブラリの脆弱性の継承

14	2022/12/6	Hirschmann 製 BAT-C2 におけるコマンドインジェクションの脆弱性	Web インタフェースの脆弱性
15	2022/12/13	Hitachi Energy 製 Lumada APM における複数の脆弱性	ライブラリの脆弱性の継承
16	2023/1/12	Moxa 製 TN-4900 シリーズにおけるハードコードされた認証情報の使用の脆弱性	認証情報の管理不備
17	2023/1/17	Campbell Scientific 製データロガーCR シリーズにおける情報漏えいの脆弱性	ネットワーク処理関連の脆弱性
18	2023/2/1	Meinberg 製 LANTIME Firemware における複数の脆弱性	ライブラリの脆弱性の継承
19	2023/2/1	Delta Electronics 製 InfraSuite Device Master における権限昇格の脆弱性	認証情報の管理不備
20	2023/2/3	Moxa 製 SDS-3008 における複数の脆弱性	Web インタフェースの脆弱性
21	2023/2/7	Siemens 製 Automation License Manager における複数の脆弱性	ネットワーク処理関連の脆弱性
22	2023/2/20	B&R 製 Automation Runtime におけるクロスサイトスクリプティングの脆弱性	Web インタフェースの脆弱性
23	2023/2/20	Hitachi Energy 製 GWS における複数の脆弱性	ライブラリの脆弱性の継承
24	2023/2/20	Phoenix Contact 製 PLCnext Firmware における複数の脆弱性	ライブラリの脆弱性の継承
25	2023/3/14	Akuvox 製 E11 における複数の脆弱性	Web インタフェースの脆弱性
26	2023/3/22	Siemens 製 SCALANCE W-700 における複数の脆弱性	ライブラリの脆弱性の継承
27	2023/3/24	Rockwell Automation 製 ThinManager ThinServer における複数の脆弱性	ネットワーク処理関連の脆弱性
28	2023/3/24	WellinTech 製 KingHistorian における複数の脆弱性	ネットワーク処理関連の脆弱性
29	2023/3/28	Meinberg 製 LANTIME Firmware における複数の脆弱性	ライブラリの脆弱性の継承

［表 2］の情報源は次のとおりです。

1. CERT@VDE | VDE-2022-047 - WAGO: FTP-Server - Denial-of-Service
   https://cert.vde.com/en/advisories/VDE-2022-047/
2. PHOENIX CONTACT | Security Advisory: Multiple Linux component vulnerabilities fixed in latest PLCnext Firmware release 2022.0.8 LTS
   https://dam-mdc.phoenixcontact.com/asset/156443151564/27f86c6f370c7d4bb45c0f57433ffcc4/Advisory_PLCnext_Linux_Components_2022.0.8_LTS.pdf
3. Meinberg | Meinberg Security Advisory: [MBGSA-2022.04] Meinberg-LANTIME-Firmware V7.06.007 and V6.24.034
   https://www.meinbergglobal.com/english/news/meinberg-security-advisory-mbgsa-2022-04-meinberg-lantime-firmware-v7-06-007-and-v6-24-034.htm
4. Tenable | Delta Electronics DIAEnergie Multiple Vulnerabilities
   https://www.tenable.com/security/research/tra-2022-33
5. Siemens | SSA-148078: Multiple Vulnerabilities in APOGEE/TALON Field Panels
   https://cert-portal.siemens.com/productcert/pdf/ssa-148078.pdf
6. JVNVU#99843134：複数の AVEVA 製品における複数の脆弱性
   https://jvn.jp/vu/JVNVU99843134/index.html
   AVEVA | SECURITY BULLETIN AVEVA-2023-001 - AVEVA™ InTouch Access Anywhere and AVEVA™ Plant SCADA Access Anywhere: Multiple Vulnerabilities
   https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2023-001_r.pdf
7. BELDEN | Multiple Java SE vulnerabilities in Belden/Hirschmann software products
   https://dam.belden.com/dmm3bwsv3/assetstream.aspx?assetid=14996&mediaformatid=50063&destinationid=10016
8. ABB | ABB Flow Computer and Remote Controllers Path Traversal Vulnerability in Totalflow TCP protocol can lead to root access
   https://library.e.abb.com/public/b17396142a3d4d14ae29e351ccc974ec/Cyber%20Security%20Advisory%20CVE-2022-0902%20-%20Path%20Traversal%20Vulnerability%20in%20Totalflow%20TCP%20protocol.pdf
9. CERT@VDE | VDE-2022-045 - Pilz: PAS 4000 prone to ZipSlip
   https://cert.vde.com/en/advisories/VDE-2022-045/
10. CERT@VDE | VDE-2022-033 - Pilz: PASvisu and PMI affected by multiple vulnerabilities
    https://cert.vde.com/en/advisories/VDE-2022-033/
11. BELDEN | Multiple vulnerabilities in BAT-C2
    https://www.belden.com/dfsmedia/f1e38517e0cd4caa8b1acb6619890f5e/15087-source
12. BELDEN | TinyXML vulnerability in Hirschmann HiLCOS products
    https://www.belden.com/dfsmedia/f1e38517e0cd4caa8b1acb6619890f5e/15089-source

13. CERT@VDE | VDE-2022-037 - Festo: Multiple Festo products contain an unsafe default Codesys configuration
https://cert.vde.com/en/advisories/VDE-2022-037/
14. BELDEN | Authenticated Command Injection in Hirschmann BAT-C2
https://www.belden.com/dfsmedia/f1e38517e0cd4caa8b1acb6619890f5e/15088-source
15. JVNVU#99602271：複数の Hitachi Energy 製品における複数の脆弱性
https://jvn.jp/vu/JVNVU99602271/index.html
Hitachi Energy | OpenSSL and Zlib Related Vulnerabilities in Hitachi Energy's Lumada Asset Performance Management (APM) Product
https://search.abb.com/library/Download.aspx?DocumentID=8DBD000134
16. Moxa | TN-4900 Series Use of Hard-coded Credentials Vulnerability
https://www.moxa.com/en/support/product-support/security-advisory/tn-4900-series-use-of-hard-coded-credentials-vulnerability
17. hackplayers | CVE-2023-0321 Divulgación de información sensible en productos de Campbell Scientific
https://www.hackplayers.com/2023/01/cve-2023-0321-info-sensible-campbell.html
18. Meinberg | Meinberg Security Advisory: [MBGSA-2023.01] Meinberg-LANTIME-Firmware V7.06.009 and V6.24.035
https://www.meinbergglobal.com/english/news/meinberg-security-advisory-mbgsa-2023-01-meinberg-lantime-firmware-v7-06-009-and-v6-24-035.htm
19. Tenable | Delta Electronics InfraSuite Device Master Privilege Escalation
https://www.tenable.com/security/research/tra-2023-4
20. Moxa | SDS-3008 Series Multiple Web Vulnerabilities
https://www.moxa.com/en/support/product-support/security-advisory/sds-3008-series-multiple-web-vulnerabilities
21. Siemens | SSA-476715: Two Vulnerabilities in Automation License Manager
https://cert-portal.siemens.com/productcert/html/ssa-476715.html
22. B&R Industrial Automation | Automation Runtime Reflected Cross-Site Scripting Vulnerabilities in SDM
https://www.br-automation.com/downloads_br_productcatalogue/assets/1675607299099-en-original-1.0.pdf
23. JVNVU#98905589：Hitachi Energy 製 Gateway Station における複数の脆弱性
https://jvn.jp/vu/JVNVU98905589/index.html
24. Hitachi Energy | Multiple Open-Source Software Vulnerabilities in Hitachi Energy's Gateway Station (GWS) Product
https://search.abb.com/library/Download.aspx?DocumentID=8DBD000118
25. PHOENIX CONTACT | Security Advisory: Multiple Linux component vulnerabilities fixed in latest PLCnext Firmware release 2023.0.0 LTS
https://dam-mdc.phoenixcontact.com/asset/156443151564/a3ed221edfc7274e8d007cd84a33c4b7/Security_Advisory_PLCnext_Linux_Components_2023.0.0_LTS.pdf

26. JVNVU#97942133：Akuvox 製 E11 における複数の脆弱性
https://jvn.jp/vu/JVNVU97942133/index.html
Claroty | The Silent Spy Among Us: Modern Attacks Against Smart Intercoms
https://claroty.com/team82/research/the-silent-spy-among-us-modern-attacks-against-smart-intercoms
27. JVNVU#99752892：Siemens 製品に対するアップデート（2023 年 3 月）
https://jvn.jp/vu/JVNVU99752892/index.html
Siemens | SSA-565386: Third-Party Component Vulnerabilities in SCALANCE W-700 IEEE 802.11ax devices before V2.0
https://cert-portal.siemens.com/productcert/pdf/ssa-565386.pdf
28. JVNVU#96051973：Rockwell Automation 製 ThinManager ThinServer における複数の脆弱性
https://jvn.jp/vu/JVNVU96051973/index.html
Rockwell Automation | ThinManager Software Path Traversal and Denial-Of-Service Attack（要ログイン）
https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640
29. Cisco Talos | TALOS-2022-1674 - WellinTech KingHistorian SORBAx64.dll RecvPacket integer conversion vulnerability
https://talosintelligence.com/vulnerability_reports/TALOS-2022-1674
Cisco Talos | TALOS-2022-1683 - WellinTech KingHistorian User authentication information disclosure vulnerability
https://talosintelligence.com/vulnerability_reports/TALOS-2022-1683
30. Meinberg | Meinberg Security Advisory: [MBGSA-2023.02] LANTIME-Firmware V7.06.013
https://www.meinbergglobal.com/english/news/meinberg-security-advisory-mbgsa-2023-02-lantime-firmware-v7-06-013.htm