ICS 脆弱性分析レポート — 2022 年度上期 —

一般社団法人 JPCERT コーディネーションセンター

2023 年 2 月 2 日

JPCERT CC®

目次

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 関連製品の脆弱性情報を認識、理解する上での一助となれば幸いです。

1.2. 2022 年度上期に注目した脆弱性情報

2022 年上期（2022 年 4 月 1 日から 2022 年 9 月 30 日までの間）で公表された ICS 関連製品の脆弱性情報を見渡すと、Web インタフェースの脆弱性に関する指摘が複数見られました。

ICS 関連製品においても管理や操作をする目的で Web インタフェースを備えていることは珍しいことではありませんし、その中に脆弱性が見つかることもあるでしょう。また、そのインタフェースの実装や利用には、情報システムと同様の注意が必要とされます。たとえ脆弱性が公表されていなくても、必要なアクセス制限を施すなど、脆弱性の存在を意識した運用が適切です。

2. Web インタフェースに関連する ICS 関連の攻撃手法および対策

ICS 関連情報製品において、Web インタフェースの脆弱性をどう評価をすればよいかは、セキュリティ担当者にとって課題の一つでしょう。この評価の方法の一つとして、MITRE の ATT&CK for ICS[1]による評価を紹介したいと思います。ATT&CK for ICS は、ICS へのサイバー攻撃を 12 段階のフェーズ（Tactics）に分け、各フェーズで実施される攻撃で使用される技術・手法（Techniques）に分類したナレッジベースです。Web インタフェースの脆弱性への評価以外にも活用できます。

ATT&CK for ICS にもとづくと、 Web インタフェースを使用する攻撃は、12 段階のフェーズの中でも「初期アクセス」と「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ます。［表 1］にそれらを記載しました。

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

［表 1：Web インタフェースを使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 Aplication 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使用する場合がある。
	T0883：Internet Accessible Device 攻撃者が、意図せずにまたは適切な保護がされないままインターネットに直接接続されたシステム経由で侵入する可能性がある。
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。

この表から、ICS 関連製品の Web インタフェースは、攻撃が行われた場合の起点や妨害のポイントとなり得ると言えます。脆弱性の悪用が侵入の起点となることは、一般的な Web サーバーでもよく見られますが、後者の「応答機能の妨害（TA0107）」の視点は特徴的かと考えます。ICS 関連製品だけではなく、その先にある制御装置や HMI の不正操作など多様な妨害が可能になります。CVSS による脆弱性の深刻度は、脆弱性による直接の影響だけから評価されており、間接的に生じる影響までは考慮されていません。ICS 関連製品では「その先」の影響も意識しておくことが重要です。

ATT&CK for ICS では、Web インタフェースを使用するこれらの攻撃手法に対するリスク軽減策もまとめられています。ICS ユーザー組織の担当者はこれらの対策の実施をご検討ください。

2.1. T0819：Exploit Public-Facing Aplication 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 や独立したネットワーク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調査し、想定と異なるかどうかを確認する（M0930）

3. ICS 関連製品の脆弱性情報への対応のお願い

ICS の利用シーンでは、迅速な不具合の修正が難しいケースが珍しくありません。脆弱性への対応についても同様で運用上の課題となっていることをよく聞きます。脆弱性のシステムに対するリスクを踏まえ、それに応じた対策の実施時期や方法（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）を選択することも検討してみてください。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. 2021 年度下期に詳細分析を行った 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 年度上期に詳細な分析を行った 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詳細な分析を行った ICS 関連製品の脆弱性情報は、[表 2] のとおり 31 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詳細な分析を行いました。

[表 2：2022 年度上期に JPCERT/CC が詳細分析を行った 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	2022/04/05	複数の Rockwell Automation 製品における複数の脆弱性	ネットワーク処理など
2	2022/04/06	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など
3	2022/04/13	Phoenix Contact 製 AXC F x152 系における複数の脆弱性	ライブラリの脆弱性の継承
4	2022/04/13	Phoenix Contact 製の複数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
5	2022/04/15	Delta Controls 製 enteliTOUCH における複数の脆弱性	Web サーバー側の入力値の処理
6	2022/04/21	Bosch 製の複数の ctrlX CORE 関連製品における複数の脆弱性	ライブラリの脆弱性の継承
7	2022/04/26	Jinan USR IOT Technology 製 4G LTE 産業用 VPN ルーターにおけるハードコードされた認証情報の使用の脆弱性	アカウント管理
8	2022/05/02	Delta Electronics 製 DRAS における複数の脆弱性	ファイル読み込み処理
9	2022/04/27	PILZ 製の複数製品における複数の脆弱性	ライブラリの脆弱性の継承
10	2022/04/27	PILZ 製 PMC Programing Tool 2.x 系における複数の脆弱性	ライブラリの脆弱性の継承
11	2022/04/27	PILZ 製 PMC Programing Tool 3.x 系における複数の脆弱性	ライブラリの脆弱性の継承
12	2022/05/06	Hitachi Energy 製 GWS および FCP における複数の脆弱性	ライブラリの脆弱性の継承

No.	情報確認日	タイトル	原因箇所
13	2022/05/06	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
14	2022/05/18	コンテック製 SolarView Compact における OS コマンドインジェクションの脆弱性	Web サーバー側の入力値の処理
15	2022/05/24	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
16	2022/06/01	Korenix 製 JetPort シリーズにおける複数の脆弱性	アカウント管理
17	2022/06/03	Endress+Hauser 製の複数製品における複数の脆弱性	ライブラリの脆弱性の継承
18	2022/06/09	SICK 製 Package Analytics における複数の脆弱性	ライブラリの脆弱性の継承
19	2022/06/15	Siemens 製 SINEMA Remote Connect Server におけるクロスサイトスクリプティングの脆弱性	Web サーバー側の入力値の処理
20	2022/06/22	Phoenix Contact 製 ProConOS/ProConOS eCLR SDK および MULTIPROG における認証情報やパスワードの管理不備の脆弱性	ユーザー認証の不備
21	2022/07/01	CAREL 製 pCOWeb HVAC BACnet Gateway におけるパストラバーサルの脆弱性	Web サーバー側の入力値の処理
22	2022/07/19	Festo 製 Controller CECC-S、LK、D シリーズにおける複数の脆弱性	ライブラリの脆弱性の継承
23	2022/08/03	三菱電機製の複数の FA 製品における複数の脆弱性	ライブラリの脆弱性の継承
24	2022/08/03	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
25	2022/08/04	SICK 製 SIM シリーズ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
26	2022/08/10	AUMA 製 SIMA² Master Station における複数の脆弱性	ライブラリの脆弱性の継承
27	2022/08/24	Advantech 製 iView におけるコマンドインジェクションの脆弱性	Web サーバー側の入力値の処理
28	2022/08/23	FLIR 製 AX8 における複数の脆弱性	Web サーバー側の入力値の処理
29	2022/08/24	Keysight Technologies 製 Sensor Manager Server における複数の脆弱性	Web サーバー側の入力値の処理など
30	2022/09/07	Hitachi Energy 製 MicroSCADA Pro/X SYS600 における複数の脆弱性	ライブラリの脆弱性の継承

No.	情報確認日	タイトル	原因箇所
31	2022/09/21	Dataprobe 製 iBoot-PDU における複数の脆弱性	クラウドサービスにおけるアクセス制御の不備など

［表 2］に記載されている製品をご使用の場合、影響を受けるバージョンかどうかを確認の上、対策を検討いただけますと幸いです。