ICS 脆弱性分析レポート ― 2023 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 11 月 30 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. 2023 年度上期に注目した脆弱性情報

2023 年度上期（2023 年 4 月 1 日から 2023 年 9 月 30 日までの間）に公表された ICS 関連製品の脆弱性情報の中から「KNX Association 製品に過度に制限されたアカウントロックアウトメカニズムの脆弱性（CVE-2023-4346）」に注目し、解説します。

今回取り上げる脆弱性は、「機器へのアクセス制御に使用するパスワードを設定した後、そのパスワードを忘れてしまうとユーザーによるリセット手段がない」という KNX プロトコルの実装上の問題に起因するものです。本脆弱性を悪用すると、攻撃者はアクセス制御の機能が有効になっていない機器にアクセスし、攻撃者しか知らないパスワードを設定してアクセス制御機能を有効にすることで、正規のユーザーを機器にアクセスできなくさせることが可能です。なお、他の ICS プロトコルを使用する製品でも同様の実装がされている製品の場合、同じセキュリティリスクを抱えている可能性があります。

本文書では、KNX プロトコルを採用した製品（以下、「KNX デバイス」という。）の中でも上記のような実装がされている製品を例に解説します。ICS ユーザー組織（ビル等建物のオーナーも含む）のセキュリティ担当者は同様の実装がなされている製品を使用しているかどうかをベンダーにご相談いただき、使用している場合は本文書を参考に対策をご検討ください。

1.3. KNX デバイスについて

KNX は国際規格（ISO／IEC 14543-3）で標準化されたオープンなホーム・ビルオートメーションのプロトコルです [1]。KNX プロトコルを採用した製品（以下、「KNX デバイス」という。）は、48 カ国 500 社のメーカーで製造 [2] されており、住宅やホテル、大規模ビル、空調、再生可能エネルギー、灌漑などの制御で使用されています [3]。KNX デバイスの設定やプログラミングは、Engineering Tool Software（以下、「ETS」という。）と呼ばれる独自のエンジニアリングソフトウェアを介して行われ、一つのプロジェクトで複数のメーカーの製品を混在させてエンジニアリングが可能となっているとのことです。KNX デバイスでは、設定や制御用プログラムの転送などに KNX Association から提供されている ETS を使用しま

[1] 日本 KNX 協会
https://knx.or.jp/

[2] KNX Community – KNX Association
https://www.knx.org/knx-en/for-professionals/community/

[3] 日本 KNX 協会「KNX 概要」
https://knx.or.jp/wp-content/uploads/2020/11/knx-overview-20201109.pdf

す。ETS を介して KNX デバイスにアクセスする際に認証を求めるようにしたい場合は、ETS のプロジェクトファイルで BCU（Bus Coupling Unit）キー[4]という任意の文字列を設定した上で、KNX デバイスにプロジェクトのデータを転送する必要があります。

2. KNX デバイス関連の脆弱性

2.1. 情報が公表された経緯

2023 年 8 月 24 日、CISA より KNX Connection Authorization を使用する KNX デバイスに関する脆弱性情報[5]が公表され、公表とあわせて本脆弱性に対するリスク軽減策が提供されています。本脆弱性は海外のセキュリティベンダーから CISA に報告されたもので、同組織は本件に関する詳細情報[6]を 2021 年 12 月 20 日に公表していますが、2023 年 8 月 25 日にこの内容を更新し、CISA から本件に関する情報が公表されて CVE ID が採番されたこと、記事更新時点で DACH（ドイツ、オーストリア、スイス）地域で 16,000 台を超える影響を受けるデバイスが見つかること、2023 年においても本脆弱性を使用した攻撃の報告を受けていることなどを追記しています。

なお、本脆弱性の情報は、2023 年 8 月 25 日に JVN で公表[7]しました。

2.2. 本脆弱性に関する一次評価

2.2.1. 想定される影響

本脆弱性は「ネットワーク経由でアクセス可能な第三者（以下「遠隔の第三者」という。）によって、デバイスをロックされ、サービス運用妨害（DoS）状態にされる恐れがある脆弱性（CVE-2023-4346）」です。

2.2.2. CVSS v3 基本評価基準による評価結果

共通脆弱性評価システム（CVSS）Version 3 による本脆弱性の評価結果は［図 1］のとおりです。

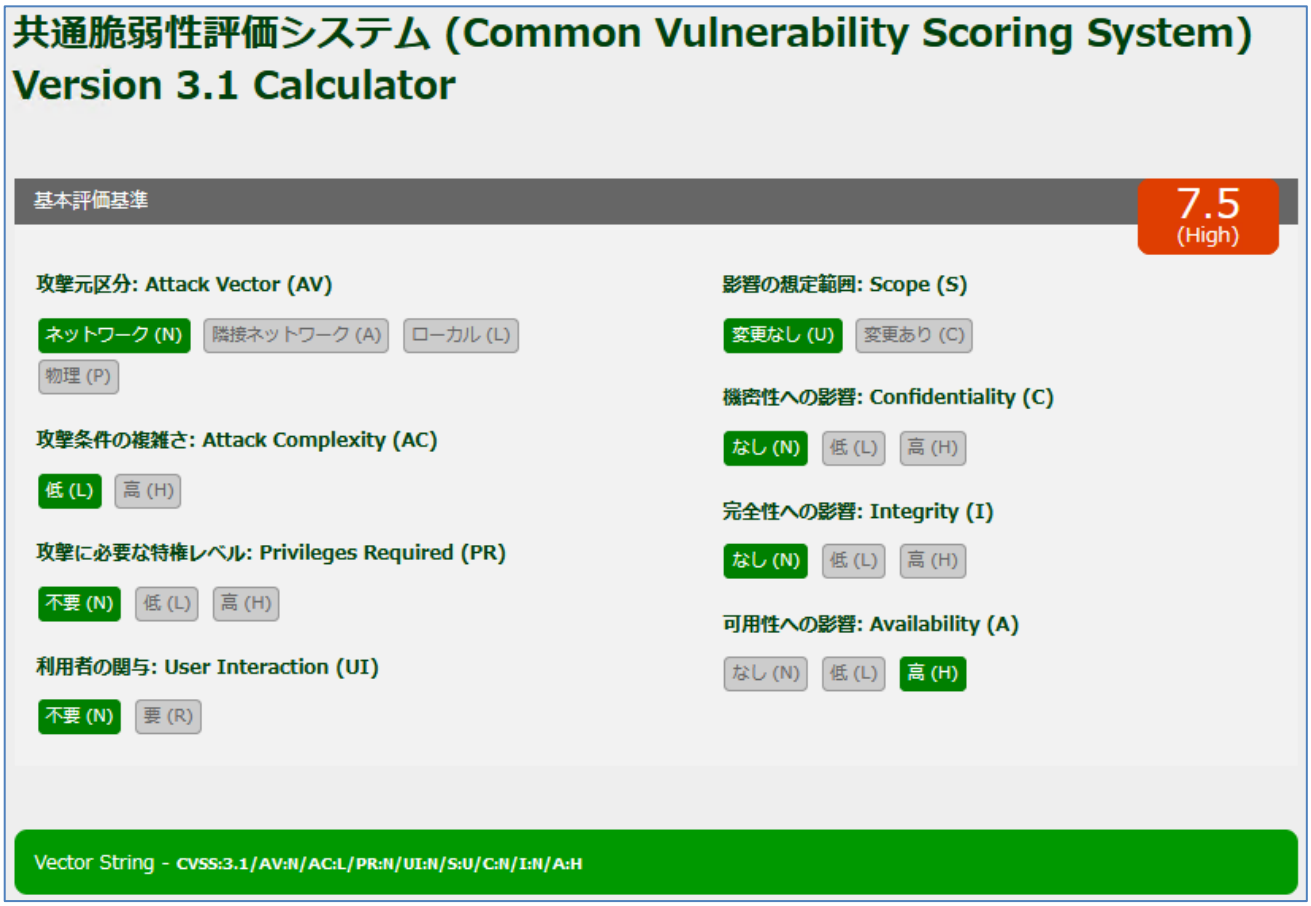
---

[4] KNX Association「Details 」
https://support.knx.org/hc/en-us/articles/115003353249-Details

[5] CISA「KNX Protocol 」
https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-01

[6] Limes Security「KNXlock – an attack campaign against KNX-based building automation systems 」
https://limessecurity.com/en/knxlock/

[7] JVN「JVNVU#92317693: KNX Association 製品に過度に制限されたアカウントロックアウトメカニズムの脆弱性」
https://jvn.jp/vu/JVNVU92317693/index.html



［図 1：共通脆弱性評価システム（CVSS）Version 3 による本脆弱性の評価結果 [8]］

本脆弱性の攻撃元区分はネットワーク（AV：N）、攻撃に必要な特権レベルは不要（PR：N）、利用者の関与は不要（UI：N）です。そのため、当該製品にアクセス可能な遠隔の第三者によって本脆弱性を使用した攻撃が行われる可能性があります。

2.2.3. 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、一次評価の判断結果

海外のセキュリティベンダーから公表された詳細情報には、本脆弱性に関する概念実証は記載されていませんでしたが、悪用事例に関する情報が記載されていました。本脆弱性は、2.2.2 に記載のとおり、遠隔の第三者によって攻撃が行われる可能性があり、本脆弱性が悪用された場合にはシステムの可用性への影響が高い（A：H）です。それを裏付ける情報として、同セキュリティベンダーの詳細情報の中で何百台もの KNX デバイスが機能しなくなったと述べられています。また、KNX プロトコルを使用する製品は国内に流通している可能性があることから、詳細を確認しました。

2.3. 本脆弱性に関する詳細確認

本脆弱性について、ビルオートメーションシステム（以下、「BAS」という。）全体への影響や想定される

[8] JVN iPedia「共通脆弱性評価システム（Common Vulnerability Scoring System）Version 3.1 Calculator」
https://jvndb.jvn.jp/cvss/ja/v31.html#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

攻撃シナリオなどについて確認しました。

2.3.1. 影響を受ける製品の詳細情報

本脆弱性は BCU キーを使用したアクセス制御の機能を有している、かつ BCU キーを忘れた場合にユーザーによるリセットする手段がない KNX デバイスが対象となっており、遠隔の（または物理アクセス可能な）第三者によって BCU キーが設定されていないデバイスにアクセスされ、BCU キーを設定されてデバイスをロックされてしまう恐れがあります。KNX Association によると、このような場合はメーカーにデバイスを返送する必要があるとのことです [9]。

なお、海外のセキュリティベンダーが対応した事例では、インターネット経由でアクセス可能になっていた本脆弱性の影響を受ける KNX デバイスが第三者によってアクセスされ、デバイスをアンロード [10]（デバイスの設定情報を削除）された上で BCU キーを設定されたため、デバイスが一切使用できなくなってしまったとのことです。また、同セキュリティベンダーが対応した範囲においては、メーカーによる BCU キーのリセットも不可能で、ハードウェアの交換を提案されたとしています。

2.3.2. 影響を受けるコンポーネントの範囲

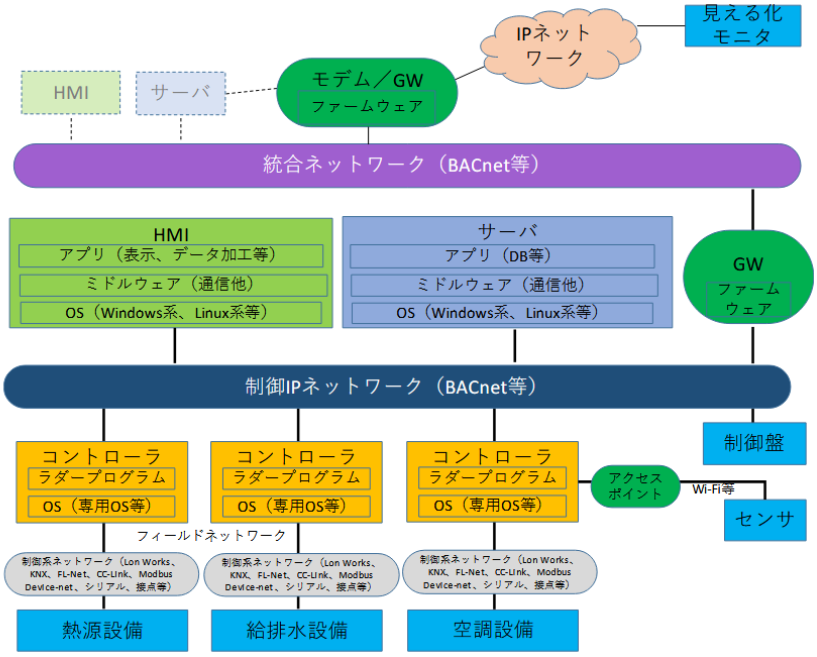
本脆弱性に関する BAS 全体への影響を確認するため、経済産業省から発行されている「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第 2 版 [11]」に示されている複数の BAS の標準的なモデルの中から「熱源・空調・給排水システムの標準的なモデル」を引用し、［図 2］に示します。

---

[9] KNX Association「BCU Key (Detailed)」
https://support.knx.org/hc/en-us/articles/360011662319

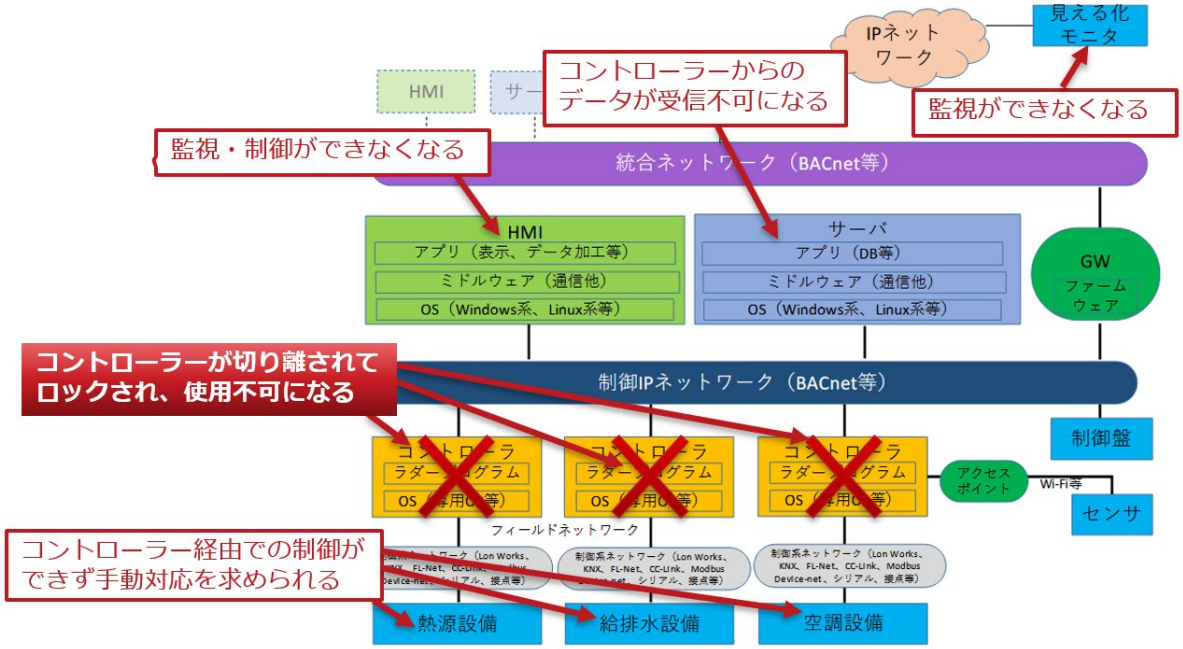
[10] KNX Association「Unload Device」
https://support.knx.org/hc/en-us/articles/4402998506386-Unload-Device

[11] 経済産業省「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第 2 版」
https://www.meti.go.jp/policy/netsecurity/wg1/bill_gideline_2.pdf



［図 2：熱源・空調・給排水システムの標準的なモデル [12]］

海外のセキュリティベンダーが対応したケースでは、KNX デバイス（コントローラー相当）がアンロードされた上でロックされてしまいました。これを踏まえると、本脆弱性を悪用した攻撃が行われた際には［図 3］のとおり、コントローラー配下の機器が制御できなくなったり、コントローラーからの情報が HMI やサーバーなどの上位のシステムに連携されなくなったりするなどの恐れがあります。



［図 3：本脆弱性における BAS 全体への想定される影響の例 [13]］

[12] 経済産業省「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第 2 版」
https://www.meti.go.jp/policy/netsecurity/wg1/bill_gideline_2.pdf

[13] 経済産業省「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第 2 版」を加工して作成
https://www.meti.go.jp/policy/netsecurity/wg1/bill_gideline_2.pdf

2.3.3. 本脆弱性を使用した想定されるシナリオ

本脆弱性を使用した攻撃が行われる場合に想定される攻撃シナリオを MITRE ATT&CK for ICS[14] (v14.1) に基づいて記載すると［表 1］のようになると考えられます。

［表 1：MITRE ATT&CK for ICS に基づく攻撃シナリオ］

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	T0883：Internet Accessible Device 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 KNX デバイスに対して攻撃が行われる。
TA0104：Execution 実行	T0823：Graphical User Interface 保護されていない KNX デバイスに対し、ETS を使用して機器の構成や設定を変更される。
TA0107：Inhabit Response Function 応答機能の妨害	T0835：Manipulate I/O Image KNX デバイスをアンロードされ、制御用プログラムやパラメーター、デバイスの構成情報などを削除される。
	T0892：Change Credential KNX デバイスへのアクセスを妨害する目的で、攻撃者によってデバイスの認証情報（BCU キー）を変更される。
TA0105：Impact 影響	T0826：Loss of Availability KNX デバイスへのアクセスが妨害され、ETS からのアクセスもできない状態になり、BAS の運用（可用性）に支障をきたす。
	T0827：Loss of Control KNX デバイスへのアクセスが妨害され、ETS からのアクセスもできない状態になり、継続的に HMI からの制御ができなくなる。
	T0829：Loss of View KNX デバイスへのアクセスが妨害され、ETS からのアクセスもできない状態になり、継続的に HMI や見える化モニタでの監視ができなくなる。

[14] MITRE ATT&CK 「ICS Matrix」
https://attack.mitre.org/matrices/ics/

2.3.4. 国内におけるインターネット経由でアクセス可能な KNX デバイス

国内における本脆弱性の影響を確認するため、インターネット経由でアクセス可能な状態になっている KNX デバイスの有無を 2023 年 8 月 25 日に調査をしました。その結果、国内ではインターネット経由でアクセス可能な状態になっている KNX デバイスは見つかりませんでした。

2.3.5. 詳細確認の結果

本脆弱性は、2.3.1 で述べたとおり、BCU キーを使用したアクセス制御の機能を有している、かつ BCU キーを忘れた場合にユーザーによるリセットする手段がない KNX デバイスに BCU キーが設定されていない場合、遠隔の第三者によって攻撃され、デバイスを使用できない状態にされてしまう可能性があります。また、本脆弱性の悪用事例が海外のセキュリティベンダーによって確認されています。JPCERT/CC が実施した調査の範囲においては、国内ではインターネット経由でアクセス可能な KNX デバイスが見つからず、直ちに攻撃につながるものではありませんでしたが、KNX デバイスは国内でも販売されており、使用されている可能性があります。

これまでの確認結果を踏まえ、上記のような実装がされている KNX デバイスを使用している場合、ICS ユーザー組織は、それが組織内外問わず、遠隔の第三者によってアクセス可能な状態になっていないか、BCU キーが未設定の状態になっていないかなどの確認と対策を検討する必要があると考えられます。

2.4. 情報提供

本脆弱性に関する情報は、2023 年 8 月 25 日に JVN で公表しています。また、一連の確認結果を踏まえると、JPCERT/CC が調査した範囲においては直ちに国内への攻撃につながるものではありません。そのため、注意喚起や参考情報などの追加情報は提供しませんでした。

2.5. ICS ユーザー組織への推奨事項

本脆弱性の影響を受ける KNX デバイスについて、KNX Association から次の推奨事項が提示されています。

- KNX Association が提供する KNX Secure Checklist[15]に記載の推奨事項に従うこと
- KNX プロジェクトが終了し、試運転が予定されている場合は必ず BCU キーを設定し、BCU キーをプロジェクト文書の一部として建物の所有者に渡すこと

また、ATT&CK for ICS では、2.3.3 で示した想定されるシナリオの攻撃手法に対するリスク軽減策がまとめられており、2.5.1 から 2.5.3 に記載しています。 ICS ユーザー組織の担当者は、2.3.1 に記載の条件

[15] KNX Association「Checklist」
https://www.knx.org/knx-en/for-professionals/benefits/knx-secure/KNX-Security-Checklist-en.pdf

に合致する KNX デバイスについて、これらの対策の実施をご検討ください。また、1.2 に記載の条件に合致する他の ICS 関連製品についても同様の対策をご検討ください。

2.5.1. 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）

2.5.2. T0892：Change Credential に対するリスク軽減策

- エンドユーザーのシステムと重要なサーバーのデータバックアップを取得し、保管する。漏えいを防止するため、バックアップシステムおよびストレージシステムを堅牢化し、組織のネットワークから分離されていることを確認する。制御、監視、または可用性に影響を及ぼす攻撃からの迅速な復旧と対応を可能にするため、主要システムのゴールデンコピーと構成の管理を含むインシデント対応計画を維持し、実施する（M0953）
- デフォルトのユーザー名とパスワードを使用するアプリケーションやアプライアンスは、インストール後速やかに、または本番環境への展開前に変更する（M0927）
- 主要なシステムが危険に晒されたり、利用できなくなったりした場合に、重要な機能の継続的な運用を保証するために、コールドスタンバイまたはそれに類似するモデルで代替ハードウェアを保持する（M0811）

2.5.3. T0826：Loss of Availability、T0827：Loss of Control、T0829：Graphical User Interface に対するリスク軽減策

- エンドユーザーのシステムと重要なサーバーのデータバックアップを取得し、保管する。漏えいを防止するため、バックアップシステムおよびストレージシステムを堅牢化し、組織のネットワークから分離されていることを確認する。制御、監視、または可用性に影響を及ぼす攻撃からの迅速な復旧と対応を可能にするため、主要システムのゴールデンコピーと構成の管理を含むインシデント対応計画を維持し、実施する（M0953）
- 特にネットワーク停止からの復旧の際に、運用プロセスの監視と制御をサポートするために、オペレーターに冗長な帯域外通信を提供する。帯域外通信は、通信インフラ内の一般的な故障モードや脆弱性を最小化するために、多様なシステムや技術を使用すべきである。例えば、無線ネットワーク（3G、4G など）は、データの多様で冗長な配信を提供するために使用できる（M0810）
- さまざまな場所でホットスタンバイを構成し、主要なシステムが危険に晒されたり、利用できなくなったりした場合でも継続的なオペレーションを保証する。ネットワーク層では、Parallel Redundancy Protocol のようなプロトコルを使用して、ローカルネットワーク上で同時に冗長化された、さまざまな通信を使用することができる（M0811）

※ 2.5.1 から 2.5.3 は MITRE 「Techniques Addressed by Mitigation」をもとに JPCERT/CC にて翻訳

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/

なお、「付録 A. 2023 年度上期に確認した 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. 2023 年度上期に確認した ICS 関連製品の脆弱性情報

2023 年度上期に 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 27 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 2：2023 年度上期に 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	2023/04/06	コンテック製 CONPROSYS HMI System（CHS）における SQL インジェクションの脆弱性	Web インタフェースの脆弱性
2	2023/04/18	複数の Schneider Electric 製品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
3	2023/04/18	SICK 製 Flexi Soft および Flexi Classic Gateways における非推奨または廃止された機能の使用の脆弱性	非推奨または廃止された機能の使用
4	2023/04/18	Franklin Fueling Systems 製 TS-550 に情報漏えいの脆弱性	Web インタフェースの脆弱性
5	2023/04/26	Schneider Electric（APC）製 Easy UPS Online Monitoring Sotware における OS コマンドインジェクションの脆弱性	Java RMI インタフェースの脆弱性
6	2023/05/02	Genetec 製 Security Center における複数の脆弱性	OS の脆弱性の継承
7	2023/05/02	Hitachi Energy 製 Modular Switchgear Monitoring（MSM）における複数の脆弱性	ライブラリの脆弱性の継承
8	2023/05/15	Schneider Electric 製 Power SCADA Anywhere における複数の脆弱性	OEM 製品の脆弱性、ライブラリの脆弱性の継承
9	2023/05/15	Advantech EKI-15XX シリーズ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
10	2023/06/29	BELDEN 製 HiSecOS における権限昇格の脆弱性	Web インタフェースの脆弱性
11	2023/06/29	Siemens 製 SIMATIC S7-1200 におけるクロスサイトリクエストフォージェリの脆弱性	Web インタフェースの脆弱性
12	2023/06/29	CODESYS を使用する複数の Eaton 製品における複数の脆弱性	ライブラリの脆弱性の継承
13	2023/06/29	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

No.	情報確認日	タイトル	原因箇所
14	2023/07/13	Siemens 製 A8000 シリーズにおける複数の脆弱性	Web インタフェース、シリアルコンソールの脆弱性
15	2023/07/25	ABB 製 Flow-X における情報漏えいの脆弱性	Web インタフェースの脆弱性
16	2023/08/01	Advantech 製 iView における SQL インジェクションの脆弱性	Web インタフェースの脆弱性
17	2023/08/01	Hirschmann 製 HiSecOS における Null ポインタ参照の脆弱性	ライブラリの脆弱性の継承
18	2023/08/01	B&R 製 Automation Runtime における制限または調整なしのリソースの割り当ての脆弱性	ネットワーク通信の処理の問題
19	2023/08/01	Hitachi Energy 製 AFF66x 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
20	2023/08/09	Phoenix Contact 製 PLCNext Engineer における複数の脆弱性	ライブラリの脆弱性の継承
21	2023/08/15	Advantech 製 EKI-152x シリーズにおける複数の脆弱性	Web インタフェースの脆弱性
22	2023/08/16	複数の Softing Industrial 製品における複数の脆弱性	入力値の検証不備
23	2023/08/22	Rockwell Automation 製 ThinManager ThinServer における複数の脆弱性	入力値の検証不備
24	2023/08/24	KNX Association 製品に過度に制限されたアカウントロックアウトメカニズムの脆弱性	ICS プロトコルの実装上の問題
25	2023/08/31	SICK 製 LMS5xx シリーズにおける複数の脆弱性	ネットワーク通信の処理の問題
26	2023/09/07	Moxa 製 MXSecurity における複数の脆弱性	Web インタフェースの脆弱性
27	2023/09/18	PTC 製 Codebeamer 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

［表 2］の情報源は次のとおりです。

1. JVN「JVNVU#92145493 コンテック製 CONPROSYS HMI System(CHS)における SQL インジェクションの脆弱性」
   https://jvn.jp/vu/JVNVU92145493/
   株式会社コンテック「 Web HMI / SCADA ソフトウェア CONPROSYS HMI System (CHS)の脆弱性について」
   https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_chs_230331_jp.pdf
   Tenable「Contec CONPROSYS HMI System (CHS) Unauthenticated SQLi」
   https://www.tenable.com/security/research/tra-2023-14
2. Schneider Electric「KNX Systems Publicly Available Exploit」
   https://download.schneider-electric.com/files?p_Doc_Ref=SESB-2023-01&p_File_Name=SESB-2023-01.pdf
3. SICK「Use of Telnet in multiple SICK Flexi Soft and Flexi Classic Gateways」
   https://sick.com/.well-known/csaf/white/2023/sca-2023-0002.pdf
4. JVN「JVNVU#93518708 Franklin Electric 製 T5 シリーズにおける強度が不十分なパスワードハッシュの使用の脆弱性」
   https://jvn.jp/vu/JVNVU93518708/index.html
   Packet Strom「Franklin Fueling Systems TS-550 Information Disclosure」
   https://packetstormsecurity.com/files/171765/Franklin-Fueling-Systems-TS-550-Information-Disclosure.html
5. Tenable「Schneider Electric APC Easy UPS Online Monitoring Software Unauthenticated RMI Calls」
   https://www.tenable.com/security/research/tra-2023-15
   Schneider Electric「Easy UPS Online Monitoring Software」
   https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_File_Name=SEVD-2023-101-04.pdf
6. Genetec「Microsoft Windows MSMQ vulnerabilities affecting Security Center」
   https://resources.genetec.com/security-advisories/microsoft-windows-msmq-vulnerabilities-affecting-security-center
7. Hitachi Energy「Multiple Open-Source Software Related Vulnerabilities in Hitachi Energy's MSM Product」
   https://publisher.hitachienergy.com/preview?DocumentID=8DBD000154&LanguageCode=en&Action=Launch
8. Schneider Electric「Power SCADA Anywhere」
   https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-129-04&p_File_Name=SEVD-2023-129-04.pdf
9. Packet Strom「Advantech EKI-15XX Series Command Injection / Buffer Overflow」
   https://packetstormsecurity.com/files/172307/Advantech-EKI-15XX-Series-Command-Injection-Buffer-Overflow.html

10. Belden「HiSecOS Web Server vulnerability allows User Role Privilege」
https://assets.belden.com/m/4828b7cf8b652105/original/Microsoft-Word-Belden_Security_Bulletin_BSECV-2021-07_1v0-docx.pdf
EXPLOIT DATABASE「HiSecOS 04.0.01 - Privilege Escalation」
https://www.exploit-db.com/exploits/51537
11. Siemens「SSA-134003: Web Vulnerability in SIMATIC S7-1200 Family」
https://cert-portal.siemens.com/productcert/pdf/ssa-134003.pdf
Packet Strom「Siemens SIMATIC S7-1200 Cross Site Request Forgery」
https://packetstormsecurity.com/files/172315/Siemens-SIMATIC-S7-1200-Cross-Site-Request-Forgery.html
12. EATON「ETN-SB-2022-1004: CODESYS SECURITY ADVISORY」
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/ETN-SB-2022-1004.pdf
13. Meinberg「Meinberg Security Advisory: [MBGSA-2023.03] LANTIME Firmware V7.06.014」
https://www.meinbergglobal.com/english/news/meinberg-security-advisory-mbgsa-2023-03-lantime-firmware-v7-06-014.htm
14. SEC Consult「Multiple Vulnerabilities including Unauthenticated Remote Code Execution in Siemens A8000」
https://sec-consult.com/vulnerability-lab/advisory/multiple-vulnerabilities-siemens-a8000
Siemens「SSA-472454: Command Injection Vulnerability in CPCI85 Firmware of SICAM A8000 Devices」
https://cert-portal.siemens.com/productcert/html/ssa-472454.html
Siemens「SSA-731916: Multiple Vulnerabilities in CPCI85 Firmware of SICAM A8000 Devices」
https://cert-portal.siemens.com/productcert/html/ssa-731916.html
15. ABB「Flow-X disclosure of sensitive information to unauthenticated users」
https://library.e.abb.com/public/442d63c231484fc98d8e7fdd46a83311/ABB-FlowX-Vulnerability-CVE-2023-1258.pdf
EXPLOIT DATABASE「ABB FlowX v4.00 - Exposure of Sensitive Information」
https://library.e.abb.com/public/442d63c231484fc98d8e7fdd46a83311/ABB-FlowX-Vulnerability-CVE-2023-1258.pdf
16. Tenable「Authenticated SQL Injection in Advantech iView」
https://www.tenable.com/security/research/tra-2023-24
17. Belden「net-snmp vulnerability in Hirschmann HiSecOS」
https://assets.belden.com/m/7a85f7945bf0ac34/original/Belden_Security_Bulletin_BSECV-2022-16.pdf
18. B&R「B&R Automation Runtime SYN Flooding Vulnerability in Portmapper」
https://www.br-automation.com/downloads_br_productcatalogue/assets/1689787619746-en-original-1.0.pdf
19. Hitachi Energy「Multiple vulnerabilities in Hitachi Energy's AFF66x Products」
https://publisher.hitachienergy.com/preview?DocumentID=8DBD000167&LanguageCode=en&Action=Launch

20. CERT@VDE「PHOENIX CONTACT: PLCnext Engineer Vulnerabilities in LibGit2Sharp/LibGit2」
https://cert.vde.com/en/advisories/VDE-2023-016/
Phoenix Contact「Security Advisory for PLCnext Engineer」
https://dam-mdc.phoenixcontact.com/asset/156443151564/1d4b504be44660448114042c376e31e6/Security_Advisory-PLCnext_Engineer_20230808.pdf
21. JVN「JVNVU#99208910 Advantech 製 EKI-1524-CE シリーズなどにおける複数のクロスサイトスクリプティングの脆弱性」
https://jvn.jp/vu/JVNVU99208910/index.html
Packet Storm「Advantech EKI-1524-CE / EKI-1522 / EKI-1521 Cross Site Scripting」
https://packetstormsecurity.com/files/174153/advantecheki12-xss.txt
22. Zero Day Initiative「(0Day) (Pwn2Own) Softing edgeConnector Siemens OPC UA Server Null Pointer Dereference Denial-of-Service Vulnerability」
https://www.zerodayinitiative.com/advisories/ZDI-23-1054/
Zero Day Initiative「(0Day) (Pwn2Own) Softing edgeAggregator Client Cross-Site Scripting Remote Code Execution Vulnerability」
https://www.zerodayinitiative.com/advisories/ZDI-23-1057/
Zero Day Initiative「(0Day) (Pwn2Own) Softing edgeAggregator Restore Configuration Directory Traversal Remote Code Execution Vulnerability」
https://www.zerodayinitiative.com/advisories/ZDI-23-1058/
Zero Day Initiative「(0Day) (Pwn2Own) Softing edgeAggregator Permissive Cross-domain Policy with Untrusted Domains Remote Code Execution Vulnerability」
https://www.zerodayinitiative.com/advisories/ZDI-23-1059/
Zero Day Initiative「(0Day) (Pwn2Own) Softing Secure Integration Server Exposure of Resource to Wrong Sphere Remote Code Execution Vulnerability」
https://www.zerodayinitiative.com/advisories/ZDI-23-1060/
Zero Day Initiative「(0Day) (Pwn2Own) Softing Secure Integration Server OPC UA Gateway Directory Creation Vulnerability」
https://www.zerodayinitiative.com/advisories/ZDI-23-1061/
Zero Day Initiative「(0Day) (Pwn2Own) Softing Secure Integration Server FileDirectory OPC UA Object Arbitrary File Creation Vulnerability」
https://www.zerodayinitiative.com/advisories/ZDI-23-1062/
Zero Day Initiative「(0Day) (Pwn2Own) Softing Secure Integration Server Interpretation Conflict Remote Code Execution Vulnerability」
https://www.zerodayinitiative.com/advisories/ZDI-23-1063/
Zero Day Initiative「(0Day) Softing Secure Integration Server Hardcoded Cryptographic Key Information Disclosure Vulnerability」
https://www.zerodayinitiative.com/advisories/ZDI-23-1064/

23. JVN「JVNVU#94607426: Rockwell Automation 製 ThinManager ThinServer における不適切な入力確認の脆弱性」
https://jvn.jp/vu/JVNVU94607426/index.html
Rockwell Automation「ThinManager® ThinServer™ Input Validation Vulnerabilities」
https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140471
Tenable「Rockwell Automation ThinManager ThinServer Multiple Vulnerabilities」
https://www.tenable.com/security/research/tra-2023-28
24. JVN「JVNVU#92317693 KNX Association 製品に過度に制限されたアカウントロックアウトメカニズムの脆弱性」
https://jvn.jp/vu/JVNVU92317693/index.html
CISA「KNX Protocol」
https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-01
25. SICK「Vulnerabilities in SICK LMS5xx」
https://sick.com/.well-known/csaf/white/2023/sca-2023-0007.pdf
26. Moxa「MXsecurity Series Multiple Vulnerabilities」
https://www.moxa.com/en/support/product-support/security-advisory/mpsa-230403-mxsecurity-series-multiple-vulnerabilities
Tenable「Moxa MXsecurity Unauthenticated Device Registration」
https://www.tenable.com/security/research/tra-2023-30
27. JVN「JVNVU#96671664 PTC 製 Codebeamer におけるクロスサイトスクリプティングの脆弱性」
https://jvn.jp/vu/JVNVU96671664/
SEC Consult「Reflected Cross-Site Scripting (XSS) in Codebeamer (ALM Solution) by PTC」
https://sec-consult.com/vulnerability-lab/advisory/reflected-cross-site-scripting-xss-in-codebeamer-alm-solution-by-ptc/
Packet Strom「PTC - Codebeamer Cross Site Scripting」
https://packetstormsecurity.com/files/174703/PTC-Codebeamer-Cross-Site-Scripting.html