ICS 脆弱性分析レポート — 2021 年度下期 —

一般社団法人 JPCERT コーディネーションセンター

2022 年 6 月 28 日

JPCERT CC®

目次

1. はじめに

1.1. 本文書の目的

本文書は、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的確に理解するために必要な知識を身に付けていただくため、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、類似した脆弱性がしばしば見られる、あるいは非常に重要な脆弱性に関するものであって、初心者にとって理解が難しいと思われる内容を含むものを選び、その内容や制御システム全体への影響などを詳細に解説したものです。

1.2. 2021 年度下期に注目した脆弱性情報

2021 年度下期に公表された ICS 関連製品の脆弱性情報の中から、CODESYS の脆弱性（CVE-2021-34593）に注目し、解説しています。

CODESYS は、CODESYS 社が提供する PLC 上のアプリケーション記述言語であるラダーロジックやファンクションブロックなどのインタープリターを中心としたライブラリ群です。CODESYS 社は、このライブラリを中核としたソフトウェア PLC や CODESYS を使って作られた PLC およびソフトウェア PLC に対応したエンジニアリングツール CODESYS Control なども製品として提供しています。

今回取り上げる脆弱性は CODESYS v2.x 系のライブラリと CODESYS Control 間の通信の処理の実装上の問題に起因するものです。

CODESYS は、400 社を超える ICS 機器ベンダーで採用されている[1]ため、さまざまな ICS 機器ベンダーの製品が本脆弱性の影響を受ける可能性があります。また、CODESYS 社から本脆弱性に対応したアップデートが提供されても、それが CODESYS で動作する PLC に適用されるまでには時間を要するため、本脆弱性の影響が長期間にわたる可能性があります。

ICS ユーザー組織のセキュリティ担当者の方は、自組織の ICS 環境に CODESYS で動作する PLC があるかどうかをベンダーにお問い合わせいただき、本脆弱性の影響を受ける製品を使用している場合は本文書を参考に対策をご検討いただけますと幸いです。

---

1 CODESYS Inside | CODESYS
https://www.codesys.com/the-system/codesys-inside.html

2. CODESYS v2.x 系のライブラリ関連の脆弱性

2.1. 情報が公表された経緯

2021 年 10 月 18 日、CODESYS 社より CODESYS v2.x 系のライブラリに関する脆弱性情報[2]が公表され、10 月 25 日に本脆弱性に対応したアップデートが提供されました。その後、2021 年 11 月 16 日に CERT@VDE から本脆弱性の影響を受ける WAGO 社の PLC の情報[3]が公表されました。CERT@VDE が公表した情報では、WAGO 社からのアップデートの提供予定は 2022 年 1 月となっており、リスク軽減策のみ提供されていました。そして、2022 年 1 月 26 日に WAGO 社のアップデートの公表とあわせて、海外セキュリティ組織から本脆弱性の概念実証を含む詳細情報[4]が公表されました。なお、本脆弱性の影響を受ける製品に関する情報については、レポート公表時点において WAGO 社以外の ICS ベンダーからは公表されていません。

2.2. 本脆弱性に対する簡易分析

2.2.1. 想定される影響

本脆弱性は「影響を受ける製品に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」）によって、サービス運用妨害（DoS）状態にされる恐れがある脆弱性（CVE-2021-34593）」です。

2.2.2. CVSS v3 基本評価基準による評価結果

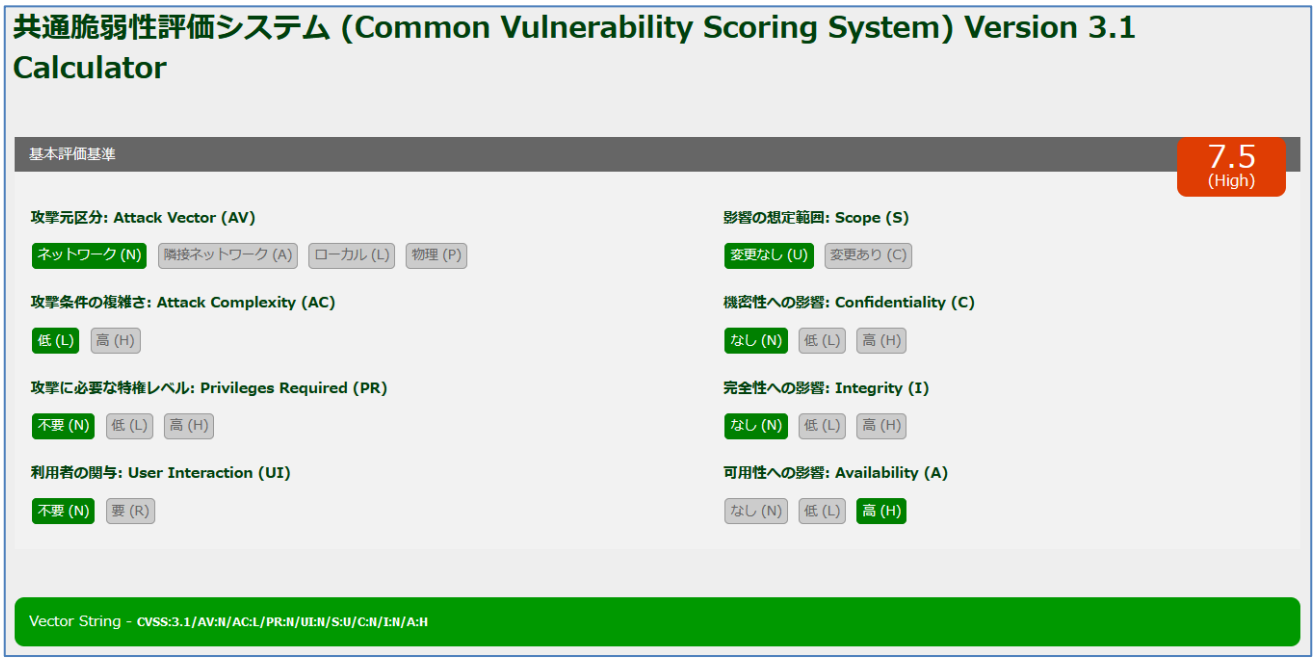
共通脆弱性評価システム（CVSS）Version 3 による本脆弱性の評価結果は図 1 のとおりです。

---

2 Advisory 2021-16：Security update for CODESYS Control V2 TCP/IP communication driver｜CODESYS
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16877&token=8faab0fc1e069f4edfca5d5aba8146139f67a175

3 WAGO: Denial of Service Vulnerability in CODESYS Runtime 2.3
https://cert.vde.com/en/advisories/VDE-2021-049/

4 Denial of service & User Enumeration in WAGO 750-8xxx PLC｜SEC Consult
https://sec-consult.com/vulnerability-lab/advisory/denial-of-service-user-enumeration-in-wago-750-8xxx-plc/



［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[5]］

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、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、簡易分析の結論

2022 年 1 月 26 日に海外セキュリティ組織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が記載されており、攻撃への転用が容易な状況になっていました。また、2.2.2 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、本脆弱性を悪用した攻撃が行われた場合にシステムの可用性への影響が高い（A：H）です。さらに、影響を受ける製品は国内でも流通が認められていること、CODESYS v2.x 系のランタイムを使用する他社製品でも本脆弱性の影響を受ける恐れがあることから、詳細な分析を行いました。なお、CODESYS 社からは本脆弱性に対応したアップデートやリスク軽減策が提供されていますが、この脆弱性に対応した ICS ベンダーは WAGO 社のみです。

2.3. 本脆弱性に対する詳細分析

詳細分析では、脆弱性の具体的な ICS への影響や攻撃シナリオについて分析しました。

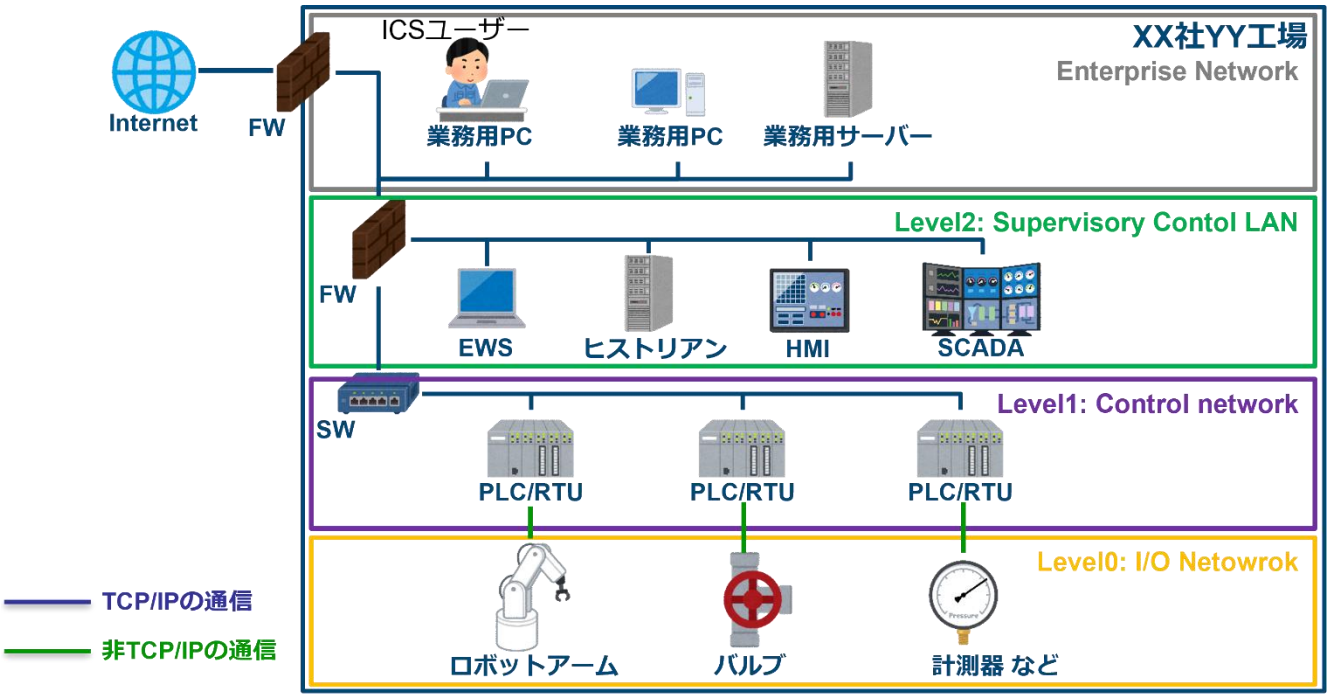
[5] 引用元：共通脆弱性評価システム (Common Vulnerability Scoring System) Version 3.1 Calculator
https://jvndb.jvn.jp/cvss/ja/v31.html#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

2.3.1. 影響を受ける製品の詳細情報、影響を受けるコンポーネントの範囲

CODESYS ライブラリで動作する PLC は、設定や制御用プログラム転送などに CODESYS 社が提供する CODESYS Control や独自のエンジニアリングツールが使用されています。

v2.4.7.56 より前のバージョンの CODESYS ライブラリで動作する PLC では、エンジニアリングツールからの通信を管理する機能に問題があり、巨大なサイズがパケットヘッダーに定義されているパケットを受信した場合にメモリ領域を確保できずに処理が中断されるものの、通信ソケットがクローズされません。そのため、遠隔の第三者によって、細工されたパケットを繰り返し送信され、PLC がエンジニアリングツールからの通信を受信できなくなってしまう恐れがあります。

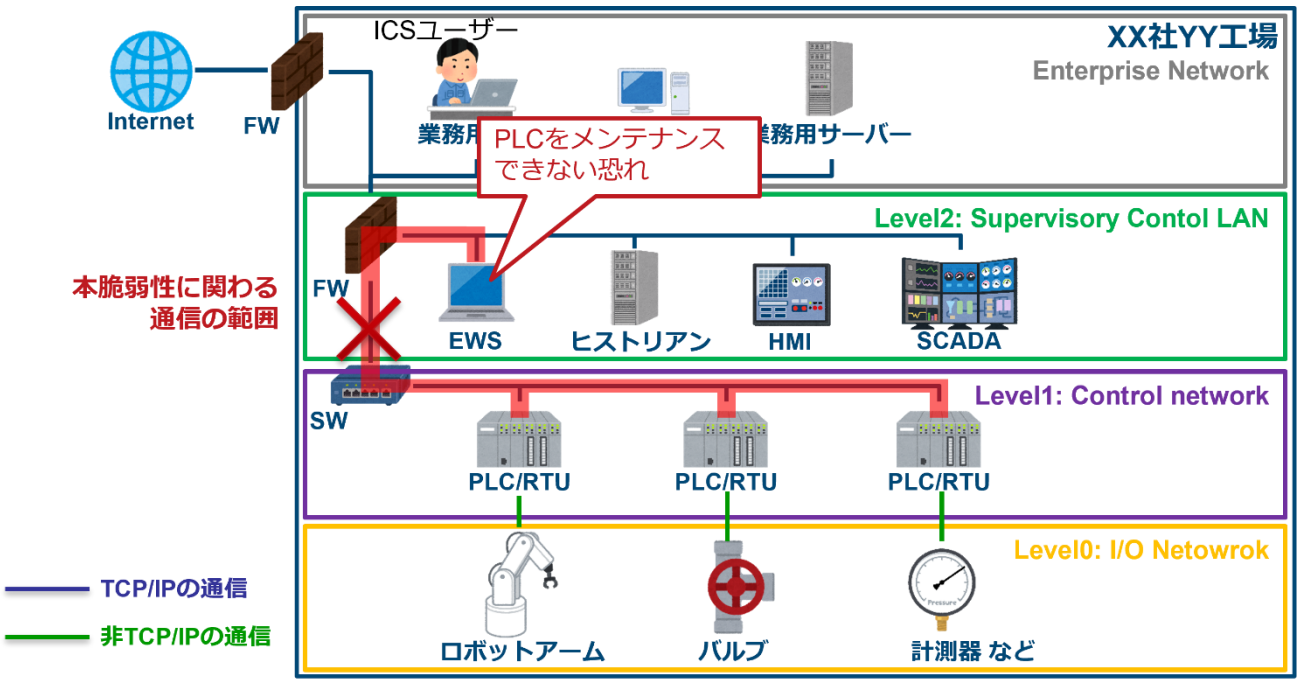
MITRE の ATT&CK for ICS では、ICS のシステム構成を 4 つの Level[6]に階層分けし、各階層に設置される ICS 製品を図 2 のとおり定義しています。Level2 と Level1 間の通信は、TCP/IP による通信が行われます。また、PLC とフィールド機器間の通信は、アナログ IO やデジタル IO、RS-485 などのシリアル接続といった非 TCP/IP での通信が行われます。



［図 2：ICS のシステム構成図（MITRE ATT&CK for ICS の定義を参考に JPCERT/CC にて作成）］

本脆弱性に関わる通信は EWS と PLC 間のものです。そのため、本脆弱性を使用した攻撃が行われると、図 3 のとおり、EWS 経由での PLC のメンテナンスができなくなる恐れがあります。

6 Levels – attackics | MITRE
https://collaborate.mitre.org/attackics/index.php/All_Levels



［図 3：本脆弱性における ICS 全体への想定される影響の例］

2.3.2. 本脆弱性を使用した想定されるシナリオ

第三者が本脆弱性を使用した攻撃を行う場合、認証不要でネットワーク越しに攻撃が可能であることから、次のような攻撃シナリオが想定されます。

(1) 意図せずインターネット経由でアクセス可能になっている PLC に対して、攻撃者が細工したパケットを送信する
(2) 攻撃者が何らかの方法（例えばリモートメンテナンス回線経由など）で Level2：Supervisory Control LAN または Level1：Control Network に侵入し、そこから PLC に対して細工したパケットを送信する など

2.3.3. インターネット経由でアクセス可能な影響を受ける製品

影響を受ける製品が意図せず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と、インターネット経由で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。そこで、国内において CODESYS で動作する PLC がインターネット経由でアクセス可能な状態になっていないかを 2022 年 2 月 7 日に調査をしました。図 4 に示す通り、104 件が確認されましたが、本脆弱性の影響を受けるバージョンであるかまでの確認はできませんでした。

［図 4：インターネット経由でアクセス可能な CODESYS で動作する PLC（2022 年 2 月 7 日時点）］

本脆弱性の影響を受ける CODESYS のライブラリは v2.4.7.56 より前のバージョンであり、確認された 104 件の中に影響を受けるバージョンの製品が含まれていると攻撃の対象となる可能性があります。

2.3.4. 詳細分析の結論

本脆弱性は、遠隔の第三者による攻撃が行われる可能性があり、なおかつ攻撃に転用可能な概念実証が公表されています。詳細分析では、インターネット経由でアクセス可能な製品が影響を受けるバージョンかどうかの特定はできませんでしたが、影響を受けるバージョンの CODESYS で動作する PLC を使用している ICS ユーザー組織は、それが外部からアクセス可能な状態になっていないか、確認と対策を検討する必要があるという結論になりました。

2.4. 情報提供

CODESYS は、国内外で広く ICS 製品の開発に使用されているライブラリです。そのため、今回の分析結果を踏まえ、CODESYS を使用して製品開発を行っていると思われる国内の ICS ベンダーに情報を提供しました。

2.5. ICS ユーザー組織への推奨事項

本脆弱性を使用した攻撃は、遠隔の第三者によって行われます。また、CODESYS で使用される通信を含む多くの制御系プロトコルは、古くから使用されていることや、ネットワークの処理速度が優先されることから、認証や通信の暗号化などのセキュリティを考慮した機能が実装されていません。そのため、本脆弱性に対するリスク軽減策は「第三者によってネットワーク経由で当該機器にアクセスされないようにすること」となり、次のような対策を推奨しています。

- 不要な場合は当該機器をインターネットから切り離す
- インターネット経由で当該機器にアクセスする場合は VPN などのセキュアな通信を使用する
  - あわせて VPN 製品に最新のセキュリティパッチが適用されていることを確認する
- ネットワーク経由での当該機器へのアクセスは必要最小限にする

- 当該機器をリモートメンテナンスする場合は外部と Level2 : Supervisory Control LAN（または Level1 : Control Network）との接続をメンテナンス作業時のみに留める　など

ICS ベンダーからアップデートが提供されている場合は、ICS への影響を ICS ベンダーに事前確認した上で適用することを推奨しています。レポート公表時点において、本脆弱性に対応したアップデートの提供は CODESYS 社および WAGO 社からのみです。今後、他の ICS ベンダーからも脆弱性情報が公表される可能性がありますので、今後の情報にもご注意ください。

3. JPCERT/CC から入手した ICS 製品の脆弱性情報への対応のお願い

ICS は、容易に停止できないかつ 1 点もののシステムであること、設備の変更管理を厳格に行う必要があることなどから、ICS ベンダーから脆弱性に対応したアップデートが提供されてもすぐに適用できません。そのため、即時の対応が必要な脆弱性については、ワークアラウンドの実施を検討することになります。脆弱性への対応の可否や優先度を決めるにあたっては、ICS ごとに影響を受ける製品がどのように設置されているかを確認した上でリスクを評価する必要があります。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、その製品がインターネットから直接アクセス可能な状態でなければ脆弱性が悪用されるリスクは下がります。

JPCERT/CC では、日本国内の影響を公開情報の範囲で調査した上で「注意喚起」を発行していますが、影響を受ける製品が実際にどのように使われているかは ICS 環境ごとに異なります。そのため、ICS ユーザー組織のセキュリティ担当者が、JPCERT/CC から提供される「注意喚起」などの脆弱性情報を収集した際には、改めて自組織の ICS 環境を踏まえた評価をいただけますと幸いです。また、日々の ICS 製品に関する脆弱性情報の収集には、JVN や ConPaS をご利用ください。

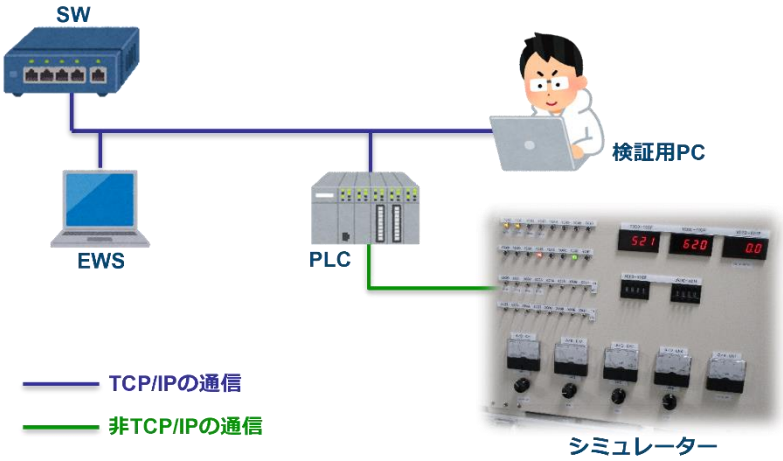
Japan Vulnerability Notes（JVN）
https://jvn.jp/
制御システムセキュリティ情報共有ポータルサイト ConPaS
https://www.jpcert.or.jp/ics/ics-community.html

なお、本文書で解説した脆弱性や「付録 B. 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」に記載されている脆弱性情報などにつきまして、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

4. 本脆弱性（CVE-2021-34593）の検証

本脆弱性の影響を確認するため、図 5 のとおり検証環境を構築しました。EWS、PLC、検証用 PC の通信は TCP/IP による通信が行われ、PLC とシミュレーター(フィールド機器の動作をシミュレートする装置)の間の通信は非 TCP/IP による通信が行われます。



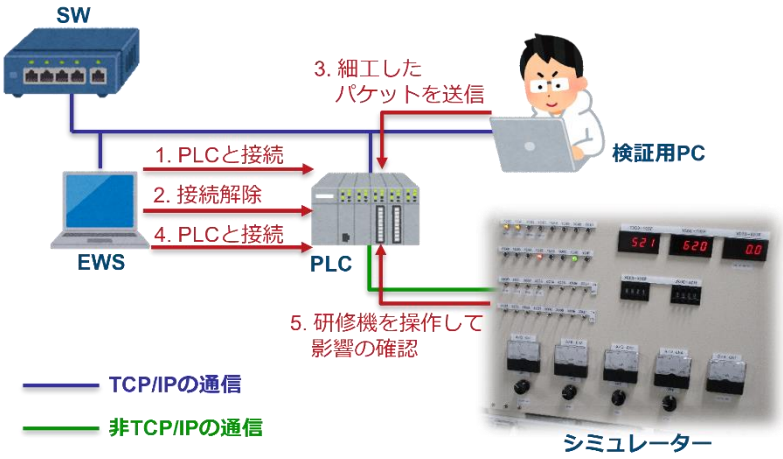
［図 5：本脆弱性の検証環境］

検証にあたっては、表に示す製品を使用しました。

- スイッチ（SW）　：NETGEAR 製 GS108Ev3
- EWS　：CODESYS v2.3.9.35
- PLC　：WAGO 製 750-841 v04.01.06（19）※CODESYS v2.3 で動作する PLC
- 検証用 PC　：Python が動作する PC
- シミュレーター　：フィールド機器の動作をシミュレートする装置

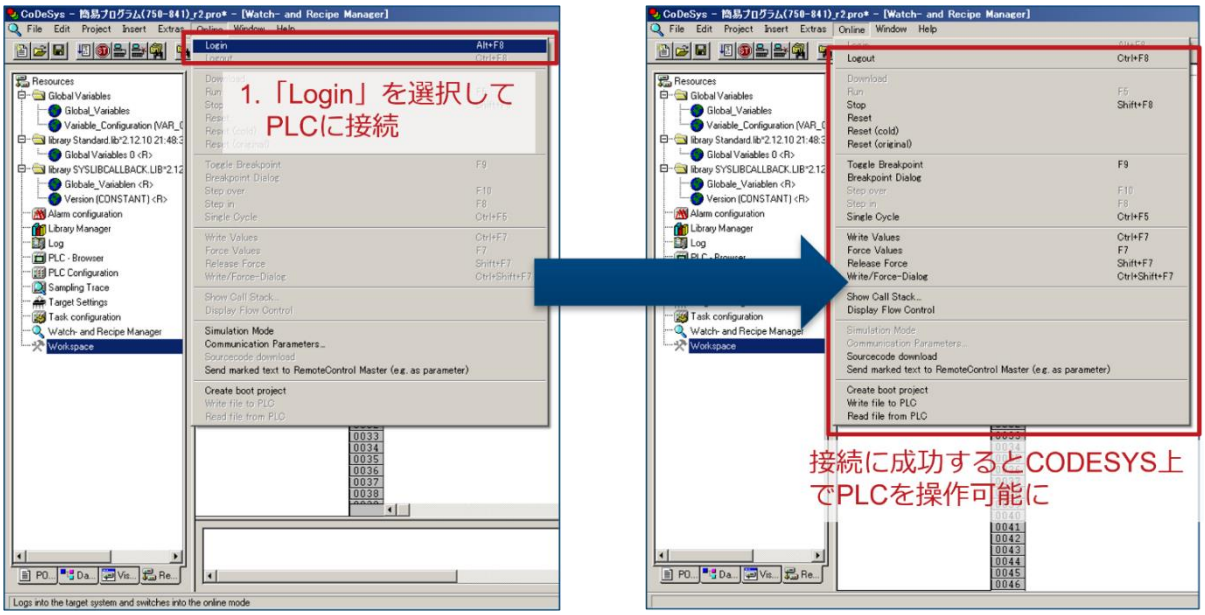
検証は図 6 に示すとおり次の手順で行いました。

(1) EWS から PLC に接続する
(2) EWS と PLC との接続を解除する
(3) 検証用 PC から CVE-2021-34593 を実証する細工したパケットを繰り返し送信する
(4) 再度 EWS から PLC への接続を試み、接続に失敗することを確認する
(5) 本脆弱性の影響を受けて、PLC とシミュレーターの間の動作に影響が出ているかどうかを確認する



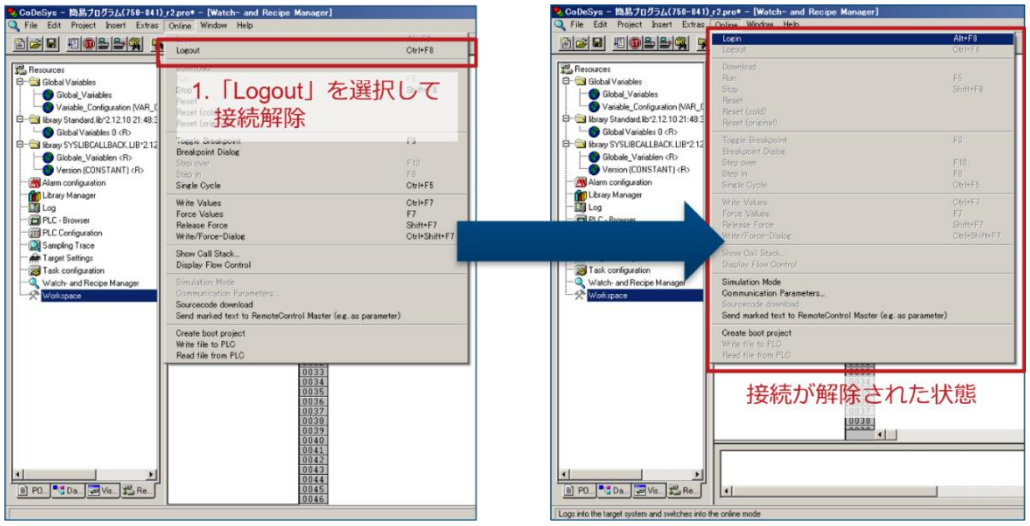
［図 6：本脆弱性の検証手順］

まず、CODESYS v2.3 を起動し、WAGO 750-841 との接続を行いました。CODESYS では、対象となる PLC との接続し、操作可能な状態にすることを「Login」と称しており、接続が成功すると、図 7 のとおり「Stop」や「Reset」などの PLC の操作が可能になります。



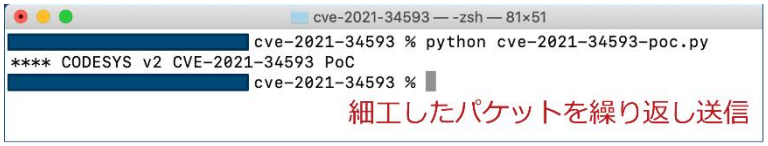
［図 7：CODESYS v2.3 から WAGO 750-841 に接続（Login）］

接続の確認が取れたため、CODESYS v2.3 と WAGO 750-841 の接続を解除します。接続の解除には、図 8 のとおり「Logout」を行います。



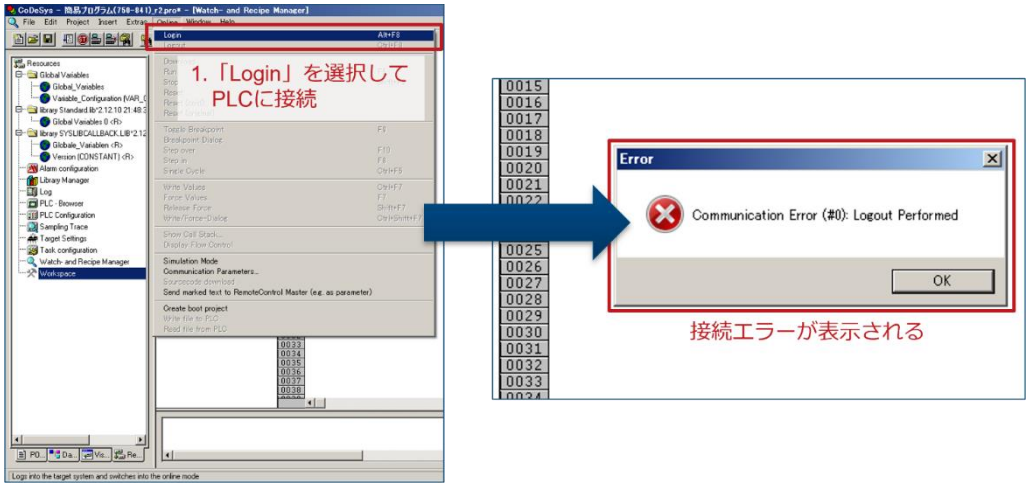
［図 8：CODESYS v2.3 と WAGO 750-841 の接続解除（Logout）］

次に、図 9 のとおり Python のスクリプトを使用して検証用 PC から本脆弱性を実証する細工したパケットを送信します。海外セキュリティ組織が公表した概念実証にもとづき、CODESYS v2.x 系ライブラリで動作する PLC に細工したパケットを繰り返し送信しました。



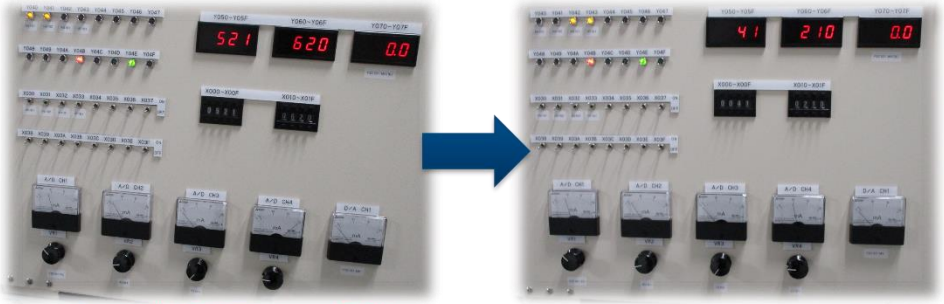
［図 9：検証用 PC から PLC に細工したパケットを繰り返し送信］

その後、改めて CODESYS v2.3 から WAGO 750-841 への接続を試みます。すると、図 10 のとおり、接続エラーが表示され、接続できなくなりました。



［図 10：細工したパケットを送信後の CODESYS v2.3 から WAGO 750-841 への再接続］

最後に、WAGO 750-841 のプログラムに影響がないことを確認します。シミュレーターを操作し、スイッチなどを操作すると、図 11 のとおり操作に追従して表示が切り替わることを確認しました。



EWSとPLCが接続不可になった直後のシミュレーターの状態

シミュレーターを操作してランプの点灯状態や数字の表示が変更された状態

［図 11：シミュレーターの操作に表示が追従することの確認］

検証の結果、PLC と TCP/IP 接続されているエンジニアリングワークステーションとの間の通信ができなくなることを確認し、2.3.1 に記載されている想定される影響の裏付けることができました。また、シミュレーターの動作には影響がなく、PLC で動作している制御用プログラムへの影響はありませんでした。なお、EWS と PLC 間の通信ができなくなってから、しばらく時間が経過した後に再度接続を試みましたが、接続不可の状態は変わらず、実機を直接操作して再起動することで EWS から PLC への接続が可能な状態に復旧しました。

付録 A. ICS 関連製品の脆弱性に関する JPCERT/CC における取り組み

一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」）では、ICS 関連製品の脆弱性情報を JVN（Japan Vulnerability Notes）[7]や制御システムセキュリティ情報共有ポータルサイト ConPaS[8]に掲載しています。これらの主な情報源は、米国 CISA[9]や JPCERT/CC が国内の ICS ベンダーと調整した案件ですが、最近では他の CERT 組織や国内および海外のセキュリティベンダー、ICS ベンダーなどからも脆弱性情報が公表されています。このような状況を踏まえ、JPCERT/CC では ICS 関連製品の脆弱性情報をインターネットなどの公開情報から積極的に収集し、深刻かつ影響範囲が広いと思われる脆弱性情報が公表された場合には、「注意喚起[10]」と呼ばれる情報を発行して利用者に広く対策を呼びかけています。また、「注意喚起」の基準に満たないものの国内で利用が認められている ICS 関連製品の脆弱性情報は、関係する ICS ユーザー組織や ICS ベンダー組織に適宜提供しています。

「注意喚起」の発行を検討する際は、脆弱性の内容や想定される影響、脆弱性の悪用が容易な状況になっていないかなど、脆弱性そのもののリスクを評価し、影響を受ける製品の日本国内での流通状況や、ICS ユーザー組織での該当製品の利用状況などを公開情報の範囲で収集、分析した上で情報提供の可否を判断しています。そのため、JPCERT/CC から公表される ICS 関連製品の「注意喚起」は、ICS ユーザー組織の担当者にもぜひ収集いただけますと幸いです。

---

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

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

9 Industrial Control Systems - CISA
https://www.cisa.gov/uscert/ics

10 注意喚起 - JPCERT/CC
https://www.jpcert.or.jp/at/2022.html

付録 B. 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

2021 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分析を行った ICS 関連製品の脆弱性情報は、表 1 のとおり 19 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」「脆弱性の存在を実証するコード（以下「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」を踏まえた簡易分析を行い、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分析を行いました。

［表 1：2021 年度下期に 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	2021/10/07	Moxa 製 MGate MB3180/MB3280/MB3480 における複数の脆弱性	ネットワークの処理
2	2021/10/13	Exacq Technologies 製 exacqVision における複数の脆弱性	アカウント管理
3	2021/10/25	富士電機製 Alpha5 のローダーソフトにおける複数の脆弱性	ファイル読み込み処理
4	2021/10/26	Mitsubishi Electric Europe B.V.製 smartRTU および INEA 製 ME-RTU における複数の脆弱性	入力値の処理など
5	2021/11/09	PEPPERL+FUCHS 製の複数の DTM 製品および VisuNet における XML 外部実体参照（XXE）に関する脆弱性	ファイル読み込み処理
6	2021/11/22	CODESYS 製 CODESYS V2 Web Server における複数の脆弱性	ネットワークの処理
7	2021/11/22	Open Degins Alliance 製 ODA Drawing SDK における複数の脆弱性	ファイル読み込み処理
8	2021/12/14	Distributed Data Systems 製 WebHMI における脆弱性における複数の脆弱性	ファイルアップロード処理
9	2021/12/15	Apache Log4j の任意のコード実行の脆弱性の影響を受ける制御システム製品に関して	入力値の処理
10	2022/02/02	Moxa 製産業用ネットワーク機器（AWK シリーズ）における複数の脆弱性	ネットワークの処理
11	2022/02/04	CODESYS 製 CODESYS PROFINET における Null ポインタ参照の脆弱性	ネットワークの処理
12	2022/02/04	WAGO 製 750-8xxx 系における複数の脆弱性	ネットワークの処理など

No.	情報確認日	タイトル	原因箇所
13	2022/02/16	Moxa 製 MXView における複数の脆弱性	ネットワークの処理など
14	2022/02/16	Moxa 製 MXView 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
15	2022/03/23	WAGO 製 750-8212 PFC200 G2 2ETH-RS における権限昇格の脆弱性	ユーザー認証
16	2022/03/23	Siemens 製 S7-1200 における重要な機能に対する認証の欠如の脆弱性	ユーザー認証
17	2022/03/24	Insyde Software 製 Insyde H2O UEFI における複数の脆弱性	メモリ操作の処理など
18	2022/03/30	APC 製 Smart-UPS における複数の脆弱性	ネットワークの処理
19	2022/03/31	Phoenix Contact 製 PROFINET SDK における複数の脆弱性	ファイル読み込み処理

2021 年度下期には、これらの詳細分析の結果から、「注意喚起」として表 2 のとおり ConPaS に掲載しました。

［表 2：ICS 関連製品の脆弱性情報の詳細分析から注意喚起の発行に至った脆弱性情報の一覧］

公表日	タイトル
2021/12/16	JPCERT-ICSAT-2021-0002: Apache Log4j の任意のコード実行の脆弱性の影響を受ける制御システム製品に関する注意喚起

また、「注意喚起」に相当する脆弱性情報ではなかったものの、ICS ユーザー組織に向けて公表すべき情報として、表 3 のとおり JVN に掲載しました。

［表 3：ICS 関連製品の脆弱性情報の詳細分析から情報提供に至った脆弱性情報の一覧］

公表日	タイトル
2021/11/25	JVNTA#94851885: Apache log4net における XML 外部実体参照（XXE）の脆弱性
2022/03/10	JVNVU#92837755: Moxa 製 MXview シリーズにおける複数の脆弱性

その他の脆弱性情報は、適宜その情報が必要と思われる組織に情報を提供しています。

表 1 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。