2012 年 11 月 2 日

独立行政法人情報処理推進機構(IPA)

【更新】ICS-ALERT-12-097-02A
3S 社 CoDeSys 不適切なアクセス制御の問題

本概要は、米国土安全保障省の運営する ICS-CERT(Industrial Control Systems Cyber Emergency Response Team)が発行する、"ICS-ALERT-12-097-02A"の抄訳となります。内容の詳細につきましては、原文をご参照ください。(※本文中のリンク先は全て英文となります)

URL: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-097-02A.pdf

概要

3S 社の CoDeSys の不適切なアクセス制御の脆弱性が一般公開された。CoDeSys は、プログラマブル・ロジック・コントローラ(PLC)やエンジニアリング用のワークステーション等で使用されるソフトウェアで、公開内容によれば、この脆弱性を悪用することにより、攻撃者は認証なしに PLC に設定ファイルをアップロードし、設定を書き換えることが可能だという。

本問題は、Digital Bond 社の Reid Wightman 氏(現在は IOActive 社)によって、ベンダおよび ICS-CERT との調整なしに公開された。

ICS-CERT では、ベンダに問題および対策の確認を依頼するとともに、注意喚起を行い、これらの脆弱性や他の攻撃によるリスクの基本的な軽減策について纏めた。

＊＊＊＊＊ 更新 A 1/2 ここから ＊＊＊＊＊

公開されたレポートでは、攻撃コードを含む 2 種のツールが公開されている。1 つは、PLC のシェルを入手するツールで、もう 1 つは、認証なしに任意のファイルを PLC と送受信するツールとなっている。

公開されたレポートでは、以下の脆弱性については、詳細を載せている。

脆弱性の種類	リモート攻撃の可否	影響
不適切なアクセス制限	可	完全性、機密性、可用性の損失
ディレクトリ・トラバーサル	可	完全性、機密性の損失

＊＊＊＊＊ 更新 A 1/2 ここまで ＊＊＊＊＊

対策

＊＊＊＊ 更新 A 2/2 ここから ＊＊＊＊＊

3S 社のウェブサイトには、CoDeSys を利用している機器を検索できるページがある。

http://www.3s-software.com/index.shtml?codesys_dev_dir （ドイツ語）
http://www.3s-software.com/index.shtml?CoDeSys_device_directory （英語）

＊＊＊＊ 更新 A 2/2 ここまで ＊＊＊＊＊

ICS-CERT では、現在、セキュリティ研究者およびベンダと対策の確認を行っている。
ICS-CERT では、ユーザはこれらの脆弱性を悪用されないために、対策を行うよう勧告する。特に、以下を行うべきである。

- 制御システム機器のネットワークへの接続を最低限に絞り込む。制御システム機器は、直接インターネットに接続しない
- ファイアウォールに守られた制御システムネットワークおよび機器を特定し、それらを業務ネットワーク（business network）から分離させる
- リモートからのアクセスが必要な場合、VPNなどセキュアな手段を用いる。但し、VPNのセキュリティの強度は、接続機器のセキュリティの高さ（弱さ）に準じることを理解したうえで検討する

なお、実際に対策を行う前に、影響分析とリスク評価を行うこと。

また、US-CERT ウェブサイト上では、他にも推奨する制御システムのセキュリティ対策を纏めたドキュメント等を提供しており、Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies（多層防御戦略による産業制御システムのサイバーセキュリティ改善）などが参照可能。

不審な活動に気づいた場合には、社の内部規定に従って対応するとともに、インシデントの把握と、他のインシデントとの関連性分析のため、ICS-CERT に報告すること。

以上