弊社 PLC の脆弱性に関するご連絡

IDEC 株式会社

公開日 2021 年 12 月 24 日
最終更新日 2021 年 12 月 24 日

■概要

弊社 PLC および、そのプログラミングソフトウェアには、不十分な認証情報の保護により、認証情報漏洩の脆弱性が存在することが判明しました。攻撃者が、通信データまたはプログラミングソフトウェアで作成したファイルから認証情報を入手することにより、PLC が不正に操作される可能性があります。
（CVE-2021-37400、CVE-2021-37401、CVE-2021-20826、CVE-2021-20827）

■CVSS スコア

CVE-2021-37400　CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L 基本値: 7.6
CVE-2021-37401　CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L 基本値: 7.6
CVE-2021-20826　CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L 基本値: 7.6
CVE-2021-20827　CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L 基本値: 7.6

■該当製品の確認方法

該当製品とソフトウェアバージョンは以下となります。

製品	ソフトウェア バージョン
FC6A 形 MICROSmart All-in-One CPU モジュール	2.32 およびそれ以前
FC6B 形 MICROSmart All-in-One CPU モジュール	2.31 およびそれ以前
FC6A 形 MICROSmart Plus CPU モジュール	1.91 およびそれ以前
FC6B 形 MICROSmart Plus CPU モジュール	2.31 およびそれ以前
FT1A 形コントローラ SmartAXIS Pro/Lite	2.31 およびそれ以前
WindLDR	8.19.1 およびそれ以前
データ ファイル マネージャー	2.12.1 およびそれ以前
WindEDIT Lite	1.3.1 およびそれ以前

■脆弱性の説明

弊社 PLC および、そのプログラミングソフトウェアには、不十分な認証情報の保護により、通信データまたはプログラミングソフトウェアで作成したファイルから認証情報が搾取される脆弱性が存在します。

■脆弱性がもたらす脅威

悪意のある攻撃者により認証情報が搾取され、PLC 内のプログラムの読み出し、書き換えなどの不正操作が行われる可能性があります。

■対策方法

対策済製品とソフトウェアバージョンは以下となります。

製品	ソフトウェア バージョン
FC6A 形 MICROSmart All-in-One CPU モジュール	2.40 およびそれ以降
FC6B 形 MICROSmart All-in-One CPU モジュール	2.40 およびそれ以降
FC6A 形 MICROSmart Plus CPU モジュール	2.00 およびそれ以降
FC6B 形 MICROSmart Plus CPU モジュール	2.40 およびそれ以降
FT1A 形コントローラ SmartAXIS Pro/Lite	2.40 およびそれ以降
WindLDR	8.20.0 およびそれ以降
データ ファイル マネージャー	2.13.0 およびそれ以降
WindEDIT Lite	1.4.0 およびそれ以降

弊社ホームページより各ソフトウェアの最新版をダウンロードしアップデートしてください。

■軽減策・回避策

本脆弱性が悪用されることによるリスクを最小限に抑えるため、専用ネットワークや VPN などの閉域網を使用してください。詳細は弊社ホームページにある「セキュリティに関する注意事項」を参照ください。https://jp.idec.com/media/jp/security-precautions.pdf

■更新履歴

2021 年 12 月 24 日　この脆弱性情報ページを公開しました。

■お問い合わせ先

弊社ホームページよりお問い合わせください。