24-R&D-0255

弊社 PLC における重要な情報の平文送信および

予測可能な ID 使用の脆弱性に関するご連絡

IDEC 株式会社

公開日 2024 年 8 月 29 日

■概要

弊社 PLC において、重要な情報の平文送信(CWE-319)および、予測可能な ID の使用(CWE-340)に関する脆弱性が存在することが判明しました。

■CVSS スコア

- 重要な情報の平文送信(CWE-319)
  - CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値 4.6
  - CVE-2024-41927
- 予測可能な ID の使用(CWE-340)
  - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L 基本値 5.3
  - CVE-2024-28957

■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	CVE
FC6A 形 MICROSmart All-in-One CPU モジュール	Ver.2.60 およびそれ以前	CVE-2024-41927 CVE-2024-28957
FC6B 形 MICROSmart All-in-One CPU モジュール	Ver.2.60 およびそれ以前	
FC6A 形 MICROSmart Plus CPU モジュール	Ver.2.40 およびそれ以前	
FC6B 形 MICROSmart Plus CPU モジュール	Ver.2.60 およびそれ以前	
FT1A 形コントローラ SmartAXIS Pro/Lite	Ver.2.41 およびそれ以前	CVE-2024-41927

■脆弱性の説明

- 重要な情報の平文送信 (CVE-2024-41927)
  攻撃者によって PLC のシリアル通信ポートから特定のコマンドを送信された場合、ユーザーの認証情報を取得される可能性があります。
- 予測可能な ID の使用 (CVE-2024-28957)
  当該製品が送信するパケットのヘッダに含まれる一部の ID を予測され、通信を妨害される可能性があります。

■脆弱性がもたらす脅威

- 重要な情報の平文送信 (CVE-2024-41927)
  通信データからユーザーの認証情報等の重要情報を取得されることにより、PLC のプログラムが取得され PLC が不正に操作される可能性があります。
- 予測可能な ID の使用 (CVE-2024-28957)
  通信パケットのヘッダに含まれる一部 ID に対して、第三者が予測した値を使用することにより通信妨害を受け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	Ver.2.70 およびそれ以降
FC6B 形 MICROSmart All-in-One CPU モジュール	Ver.2.70 およびそれ以降
FC6A 形 MICROSmart Plus CPU モジュール	Ver.2.50 およびそれ以降
FC6B 形 MICROSmart Plus CPU モジュール	Ver.2.70 およびそれ以降
FT1A 形コントローラ SmartAXIS Pro/Lite	Ver.2.50 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

- 重要な情報の平文送信(CVE-2024-41927)
  攻撃者が PLC のシリアル通信ポートに接続できないように PLC を適切に管理してください。
- 予測可能な ID の使用(CVE-2024-28957)
  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。

■更新履歴

2024 年 8 月 29 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。