弊社 PLC(CJ シリーズ CPU)に対する
外部機関からの脆弱性指摘について

オムロン株式会社

公開日 2020 年 2 月 28 日

平素はオムロン製プログラマブルコントローラ(PLC)をご愛顧いただき、まことにありがとうございます。

早速ですが、外部機関から弊社 PLC が独自に実装している FINS 通信プロトコルに対する 1 件の脆弱性を指摘されました。お客様におかれましては、下記詳細内容をご一読いただき、リスク回避のための対策をお取りいただきますようお願いいたします。

1. 影響を受ける機器

   オムロンの CJ シリーズ CPU の全バージョン

2. 脆弱性の概要

   2.1 FINS 通信プロトコルの DoS 攻撃に対する脆弱性

   ・CVE-2020-6986　FINS 不正パケットを用いた高負荷(Flooding)攻撃に対する脆弱性

   CWE：CWE-400 Uncontrolled Resource Consumption

   CVSSv3　：7.5(High)　CVSS:7.5/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   PLC(CJ シリーズ) は、過度な不正パケット処理における不適切な資源管理に関する脆弱性が存在します。

3. リスク回避のための対策

   上記のような脆弱性を突いた攻撃を受けるリスクを回避するため、従来から弊社ではお客様ご自身にて、以下の対策を講じていただくようお願いしております。

   ① アンチウイルス保護

   ② データ入出力の保護

   ③ データ復元のためのバックアップ

   ④ 弊社の製品またはインストールされたソフトウェアに対するコンピュータウイルス感染防止

   ⑤ 弊社の製品に対する不正アクセス防止についての十分な措置

   例えば、ファイアウォールによる外部ネットワークからの遮断、VPN によるネットワークアクセスの制限、ネットワーク側で Well-Known な通信ポートをフィルタリング(FINS 通信ポートはデフォルト 9600)などの適切なセキュリティ対策を行ってください。

弊社といたしましては、今後も製品のセキュリティを強化していく努力を続けてまいりますので、引き続きのご愛顧を賜りますようよろしくお願いいたします。