MELSEC-Q/L シリーズ CPU ユニットにおける情報漏えい及び悪意のあるプログラムが実行される脆弱性

公開日 2024 年 3 月 14 日
最終更新日 2024 年 5 月 16 日
三菱電機株式会社

■概要

MELSEC-Q/L シリーズの CPU ユニットには、不正なポインタの増減(CWE-468)[1]及び整数オーバーフローまたはラップアラウンド(CWE-190)[2]による、情報漏えい及び悪意のあるプログラムが実行される脆弱性が存在することが判明しました。攻撃者が該当製品に対して細工されたパケットを送信することにより、当該製品の任意の情報が読出される、または悪意のあるプログラムが実行される可能性があります。(CVE-2024-0802、CVE-2024-0803、CVE-2024-1915、CVE-2024-1916、CVE-2024-1917)

■CVSS スコア [3]

CVE-2024-0802 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:9.8
CVE-2024-0803 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:9.8
CVE-2024-1915 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:9.8
CVE-2024-1916 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:9.8
CVE-2024-1917 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値:9.8

■該当製品の確認方法

影響を受ける製品の形名、バージョンは以下のとおりです。

シリーズ	形名	バージョン
MELSEC-Q シリーズ	Q03UDECPU、Q04/06/10/13/20/26/50/100UDEHCPU	全バージョン
	Q03/04/06/13/26UDVCPU	全バージョン
	Q04/06/13/26UDPVCPU	全バージョン
MELSEC-L シリーズ	L02/06/26CPU(-P)、L26CPU-(P)BT	シリアル No.の上 5 桁"26041"以前

■脆弱性の説明

MELSEC-Q/L シリーズの CPU ユニットには、下記 5 件の脆弱性が存在します。

- CVE-2024-0802:不正なポインタの増減(CWE-468)による情報漏えい及び悪意のあるプログラムが実行される脆弱性
- CVE-2024-0803:整数オーバーフローまたはラップアラウンド(CWE-190)による悪意のあるプログラムが実行される脆弱性
- CVE-2024-1915:不正なポインタの増減(CWE-468)による悪意のあるプログラムが実行される脆弱性
- CVE-2024-1916:整数オーバーフローまたはラップアラウンド(CWE-190)による悪意のあるプログラムが実行される脆弱性
- CVE-2024-1917:整数オーバーフローまたはラップアラウンド(CWE-190)による悪意のあるプログラムが実行される脆弱性

■脆弱性がもたらす脅威

【CVE-2024-0802】

攻撃者が、該当製品に対して細工されたパケットを送信することにより、当該製品の任意の情報が読出される、または悪意のあるプログラムが実行される可能性があります。

【CVE-2024-0803、CVE-2024-1915、CVE-2024-1916、CVE-2024-1917】

攻撃者が該当製品に対して細工されたパケットを送信することにより、悪意のあるプログラムが実行される可能性があります。

■お客様での対応

該当製品・該当バージョンをご使用のお客様は、軽減策・回避策にて対応ください。

次項の通り対策済み製品をリリースしておりますが、対策版へのアップデートはできませんので、後継機種である MELSEC iQ-R シリーズへの移行もご検討ください。

■製品での対応

対策済の製品およびバージョンは、以下となります。

シリーズ	形名	バージョン
MELSEC-L シリーズ	L02/06/26CPU(-P)、L26CPU-(P)BT	シリアル No.の上 5 桁"26042"以降

[1] https://cwe.mitre.org/data/definitions/468.html
[2] https://cwe.mitre.org/data/definitions/190.html
[3] https://www.ipa.go.jp/security/vuln/CVSSv3.html

■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、三菱電機は以下に示す軽減策を講じることを推奨します。

・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止してください。

・当該製品を LAN 内で使用し、信頼できないネットワークやホストからのアクセスをファイアウォールでブロックしてください。

・当該製品並びに当該製品へ接続可能なパソコン及びネットワーク機器への物理的なアクセスを制限してください。

・当該製品へアクセス可能なパソコンにウィルス対策ソフトを搭載してください。

■謝辞

この問題をご報告いただいた Positive Technologies の Anton Dorfman 様に感謝いたします。

■お問い合わせ先

製品をご購入いただいた当社の支社、代理店にご相談ください。

〈お問い合わせ | 三菱電機 FA〉

https://www.mitsubishielectric.co.jp/fa/support/purchase/index.html

■更新履歴

2024 年 5 月 16 日

「対策方法」を「お客様での対応」と「製品での対応」に分けました。

「製品での対応」に対応済みの製品を追加しました。

L02/06/26CPU(-P)、L26CPU-(P)BT