三菱電機数値制御装置におけるサービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性

公開日 2023 年 7 月 27 日
最終更新日 2024 年 1 月 30 日
三菱電機株式会社

■概要

三菱電機数値制御装置(CNC)にサービス拒否（DoS）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。悪意のある攻撃者からの不正なパケットを受信すると、該当製品の通信機能がサービス停止(DoS)状態に陥ったり、悪意のあるプログラムを実行されたりする可能性があります。(CVE-2023-3346)

この脆弱性の影響を受ける製品形名およびバージョンを以下に示します。

■CVSS スコア [1]

CVE-2023-3346 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、システム番号及びバージョンは、以下のとおりです。

シリーズ名	製品名	システム番号 (**はバージョンを示す)	バージョン
M800V/M80V シリーズ	M800VW	BND-2051W000-**	A8 版以前
	M800VS	BND-2052W000-**	
	M80V	BND-2053W000-**	
	M80VW	BND-2054W000-**	
M800/M80/E80 シリーズ	M800W	BND-2005W000-**	FB 版以前
	M800S	BND-2006W000-**	
	M80	BND-2007W000-**	
	M80W	BND-2008W000-**	
	E80	BND-2009W000-**	
C80	C80	BND-2036W000-**	BF 版以前
M700V/M70V/E70 シリーズ	M750VW	BND-1015W002-**	LF 版以前
	M730VW/M720VW	BND-1015W000-**	
	M750VS	BND-1012W002-**	
	M730VS/M720VS	BND-1012W000-**	
	M70V	BND-1018W000-**	
	E70	BND-1022W000-**	
IoT ユニット	リモートサービスゲートウェイユニット	BND-2041W001-**	AD 版以前
	情報収集ユニット	BND-2041W002-**	全てのバージョン

M800V/M80V シリーズ、M800/M80/E80 シリーズ、C80、M700V/M70V/E70 シリーズの場合、以下の手順でシステム番号を表示し確認します。

① 表示ユニットにて「診断」画面を表示し、「構成」メニューを選択すると、ソフトウェア構成画面が表示されます。
② ソフトウェア構成画面で NCMAIN1 に表示されるシステム番号を確認します。

IoT ユニットの場合、パソコンで Web ブラウザから設定画面にログインし、ログイン後の画面に表示される S/W Version で確認します。

■脆弱性の説明

当該製品には、古典的バッファオーバーフロー(CWE-120)[2] によるサービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者からの細工された不正なパケットを受信すると、当該製品がサービス停止(DoS)状態に陥ったり、悪意のあるプログラムを実行されたりする可能性があります。なお、復旧にはシステムのリセットが必要になります。

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/120.html

■対策方法

対策済のシリーズ名、製品名、システム番号及びバージョンは以下のとおりです。

＜シリーズ名とシステム番号とバージョン＞

シリーズ名	製品名	システム番号 (**はバージョンを示す)	バージョン
M800V/M80V シリーズ	M800VW	BND-2051W000-**	A9 版以降
	M800VS	BND-2052W000-**	
	M80V	BND-2053W000-**	
	M80VW	BND-2054W000-**	
M800/M80/E80 シリーズ	M800W	BND-2005W000-**	FC 版以降
	M800S	BND-2006W000-**	
	M80	BND-2007W000-**	
	M80W	BND-2008W000-**	
	E80	BND-2009W000-**	
C80	C80	BND-2036W000-**	BG 版以降
M700V/M70V/E70 シリーズ	M750VW	BND-1015W002-**	LG 版以降
	M730VW/M720VW	BND-1015W000-**	
	M750VS	BND-1012W002-**	
	M730VS/M720VS	BND-1012W000-**	
	M70V	BND-1018W000-**	
	E70	BND-1022W000-**	
IoT ユニット	リモートサービスゲートウェイユニット	BND-2041W001-**	AE 版以降

＜対策済のバージョンの適用方法＞

対策済のバージョンの適用方法については、最寄りの三菱電機窓口までご相談ください。

■軽減策・回避策

すぐにシステムをアップデートできないお客様に対して、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。
・当該製品へアクセス可能なパソコンにウイルス対策ソフトを搭載してください。
・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。
・当該製品および当該製品が接続された LAN への物理的なアクセスを制限してください。

■謝辞

本脆弱性をご報告いただいた、ZHEJIANG QIAN INFORMATION&TECHNOLOGY CO., LTD.の 01dGu0 様に感謝いたします。

■お客様からのお問い合わせ先

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 1 月 30 日
「対策方法」に対策済機種を追加しました。
C80

2023 年 12 月 5 日
「対策方法」に対策済機種を追加しました。
リモートサービスゲートウェイユニット

2023 年 11 月 21 日
「対策方法」に対策済機種を追加しました。
M800VW、M800VS、M80V、M80VW、M750VW、M730VW/M720VW、M750VS、M730VS/M720VS、M70V、E70

2023 年 10 月 31 日
「該当製品の確認方法」の「製品名」及び「システム番号」を修正しました。
M730VS のシステム番号を修正
M750VS 15 型及び 730VS/M720VS 15 型を削除
「対策方法」に対策済機種を追加しました。
M800W、M800S、M80、M80W、E80

2023 年 8 月 3 日
「該当製品の確認方法」の「製品名」及び「システム番号」を修正しました。
M730VW/M720VW、M720VS
「該当製品の確認方法」の「製品名」及び「システム番号」を追加しました。
M750VW、M750VS、M730VS、M750VS 15 型、M730VS/M720VS 15 型