三菱電機数値制御装置におけるサービス拒否(DoS)の脆弱性

公開日 2026 年 3 月 10 日
三菱電機株式会社

■概要

三菱電機数値制御装置(CNC)において、サービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者は、TCP 683 番ポートへ不正なパケットを送信することにより、領域外のメモリ読み出しを発生させ、該当製品をサービス停止(DoS)状態に陥らせることができる可能性があります。(CVE-2025-2399)

この脆弱性の影響を受ける製品形名及びバージョンを以下に示します。

■CVSS スコア [1]

CVE-2025-2399　CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:5.9

■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-**	BB 版以前
	M800VS	BND-2052W000-**	
	M80V	BND-2053W000-**	
	M80VW	BND-2054W000-**	
M800/M80/E80 シリーズ	M800W	BND-2005W000-**	FM 版以前
	M800S	BND-2006W000-**	
	M80	BND-2007W000-**	
	M80W	BND-2008W000-**	
	E80	BND-2009W000-**	
C80 シリーズ	C80	BND-2036W000-**	すべてのバージョン
M700V/M70V/E70 シリーズ	M750VW	BND-1015W002-**	すべてのバージョン
	M730VW/M720VW	BND-1015W000-**	
	M750VS	BND-1012W002-**	
	M730VS/M720VS	BND-1012W000-**	
	M70V	BND-1018W000-**	
	E70	BND-1022W000-**	
ソフトウェアツール	NC Trainer2	BND-1802W000-**	すべてのバージョン
	NC Trainer2 plus	BND-1803W000-**	

M800V/M80V シリーズ、M800/M80/E80 シリーズ、C80 シリーズ及び M700V/M70V/E70 シリーズの場合には、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(図 1～図 4 ①参照)、「構成」メニューを選択する(図 1～図 4 ②参照)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(図 1～図 4 ③参照)を確認します。

[1] https://www.ipa.go.jp/security/vuln/CVSSv3.html

図 1. M800V/M80V シリーズのソフトウェア構成画面

図 2. M800/M80/E80 シリーズのソフトウェア構成画面

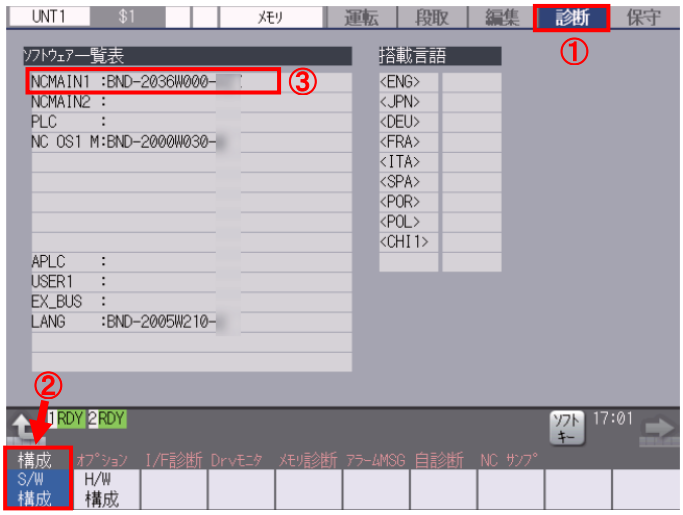

図 3. C80 シリーズのソフトウェア構成画面

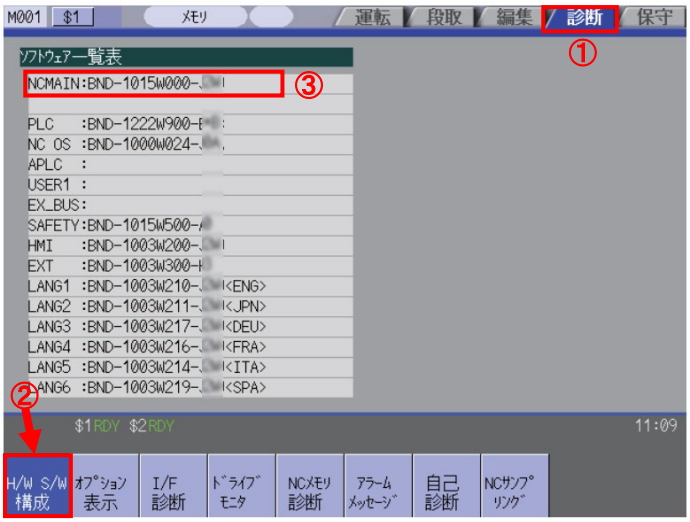

図 4. M700V/M70V/E70 シリーズのソフトウェア構成画面

NC Trainer2 及び NC Trainer2 plus の場合には、以下の手順でシステム番号を表示し、確認します。

(1) プログラムを起動します。

(2) メニューバーの「ヘルプ」(図 5 ①参照)-「バージョン情報」(図 5 ②参照)をクリックしてバージョン情報画面を表示し、BND で始まるシステム番号を確認します。(図 5 ③参照)

図 5. NC Trainer2 及び NC Trainer2 plus のバージョン情報画面

詳しくは、各製品の取扱説明書(下表)を参照ください。

シリーズ名	説明書名	参照先
M800V/M80V シリーズ	M800V/M80V シリーズ 取扱説明書	https://www.mitsubishielectric.co.jp/fa/download/index.html
M800/M80/E80 シリーズ	M800/M80/E80 シリーズ 取扱説明書	
M700V/M70V/E70 シリーズ	M700V/M70V/E70 シリーズ取扱説明書	
C80 シリーズ	C80 シリーズ 取扱説明書	
ソフトウェアツール	NC Trainer2/NC Trainer2 plus 取扱説明書	

■脆弱性の説明

当該製品には、入力で指定されたインデックス、位置、またはオフセットの不適切な検証(CWE-1285)[2]による、サービス拒否(DoS)の脆弱性が存在します。

[2] https://cwe.mitre.org/data/definitions/1285.html

■脆弱性がもたらす脅威

攻撃者は、TCP 683 番ポートへ不正なパケットを送信することにより、領域外のメモリ読み出しを発生させ、該当製品をサービス停止(DoS)状態に陥らせることができる可能性があります。該当製品がサービス停止(DoS)状態に陥ると、システムが非常停止します。なお、復旧にはシステムのリセットが必要になります。

■お客様での対応

「■製品での対応」に掲載の表を参照して、お使いの製品の対策版が提供されているかをご確認ください。

〈対策版が提供されている製品をお使いのお客様〉

対策済みバージョンを適用ください。適用方法については、最寄りの三菱電機窓口へご相談ください。

〈対策版が提供されていない製品をお使いのお客様〉

軽減策・回避策にて対応をお願いいたします。

■製品での対応

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	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-**	BC 版以降
	M800VS	BND-2052W000-**	
	M80V	BND-2053W000-**	
	M80VW	BND-2054W000-**	
M800/M80/E80 シリーズ	M800W	BND-2005W000-**	FN 版以降
	M800S	BND-2006W000-**	
	M80	BND-2007W000-**	
	M80W	BND-2008W000-**	
	E80	BND-2009W000-**	

■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、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。

・IP アドレスフィルタ機能※1を使用し、信頼できないホストからのアクセスをブロックしてください。

※1:IP アドレスフィルタ機能は、M800V/M80V シリーズと M800/M80/E80 シリーズで対応しています。
IP アドレスフィルタ機能の詳細は、M800V/M80V シリーズ取扱説明書「16. 付録 3 IP アドレスフィルタ機能」又は M800/M80/E80 シリーズ取扱説明書「15. 付録 2 IP アドレスフィルタ機能」を参照ください。

・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イルス対策ソフトを搭載してください。

■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