Denial of Service (DoS) Vulnerability in Mitsubishi Electric CNC Series

Release date: March 10, 2026
Mitsubishi Electric Corporation

Overview

A denial of service (DoS) vulnerability exists in Mitsubishi Electric Numerical Control Systems (CNC). A remote attacker may be able to cause an out-of-bounds read, resulting in a denial of service (DoS) condition in the affected products by sending specially crafted packets to TCP port 683. (CVE-2025-2399)
The product models and system versions affected by this vulnerability are listed below.

CVSS[1]

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

Affected products

The following products, System Number and Versions are affected:

Series	Product Name	System Number (**=Version)	Version
M800V/M80V Series	M800VW	BND-2051W000-**	BB and prior
	M800VS	BND-2052W000-**	
	M80V	BND-2053W000-**	
	M80VW	BND-2054W000-**	
M800/M80/E80 Series	M800W	BND-2005W000-**	FM and prior
	M800S	BND-2006W000-**	
	M80	BND-2007W000-**	
	M80W	BND-2008W000-**	
	E80	BND-2009W000-**	
C80 Series	C80	BND-2036W000-**	All versions
M700V/M70V/E70 Series	M750VW	BND-1015W002-**	All versions
	M730VW/M720VW	BND-1015W000-**	
	M750VS	BND-1012W002-**	
	M730VS /M720VS	BND-1012W000-**	
	M70V	BND-1018W000-**	
	E70	BND-1022W000-**	
Software Tools	NC Trainer2	BND-1802W000-**	All versions
	NC Trainer2 plus	BND-1803W000-**	

For M800V/M80V, M800/M80/E80, C80, and M700V/M70V/E70 Series, please check the “System Number” by following steps.

1) Open the “Diagnostics” screen on the display (see [1] in Figures 1 to 4) and select the “Config” menu (see [2] in Figures 1 to 4) to display the Software Configuration screen.
2) Check the “System Number” displayed in “NCMAIN1” on the Software Configuration screen (see [3] in Figures 1 to 4).

[1] https://www.first.org/cvss/v3.1/specification-document

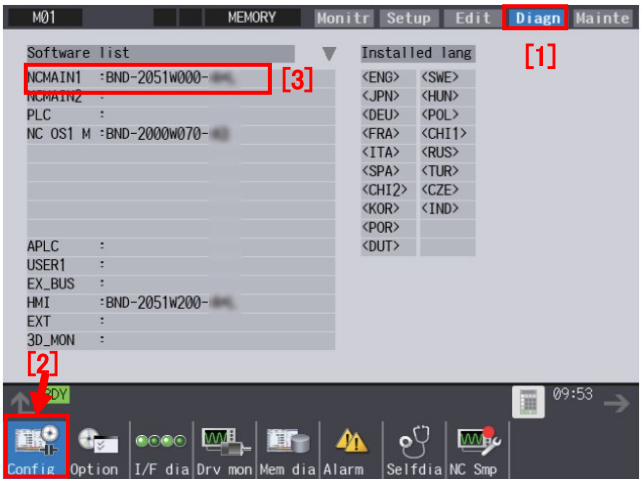

Figure 1. Software Configuration screen (800V/M80V Series)

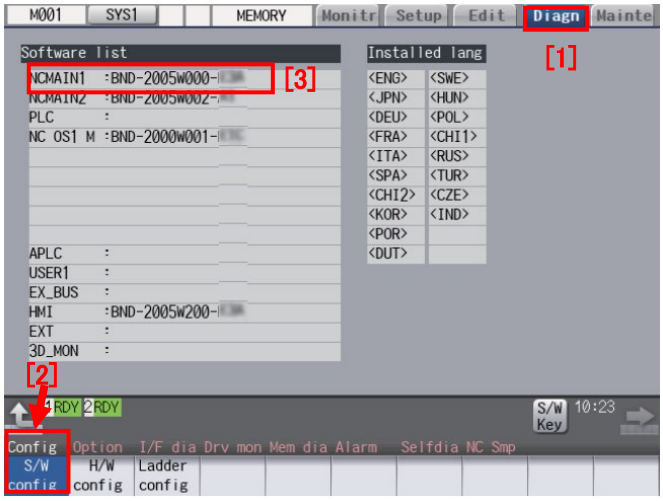

Figure 2. Software Configuration screen (M800/M80/E80 Series)

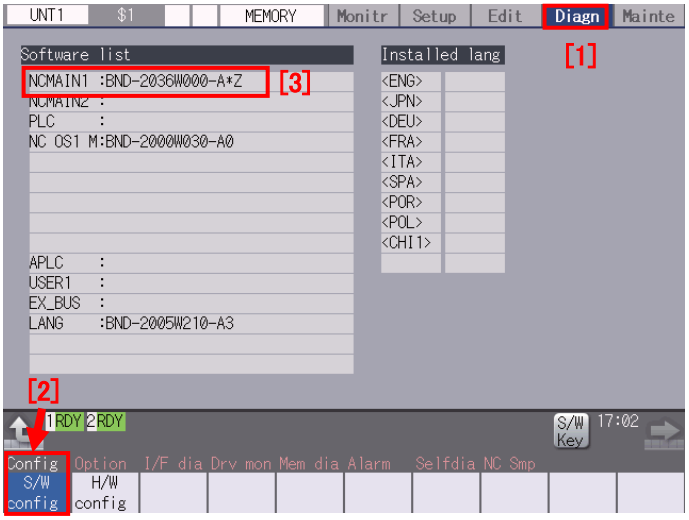

Figure 3. Software Configuration screen (C80 Series)

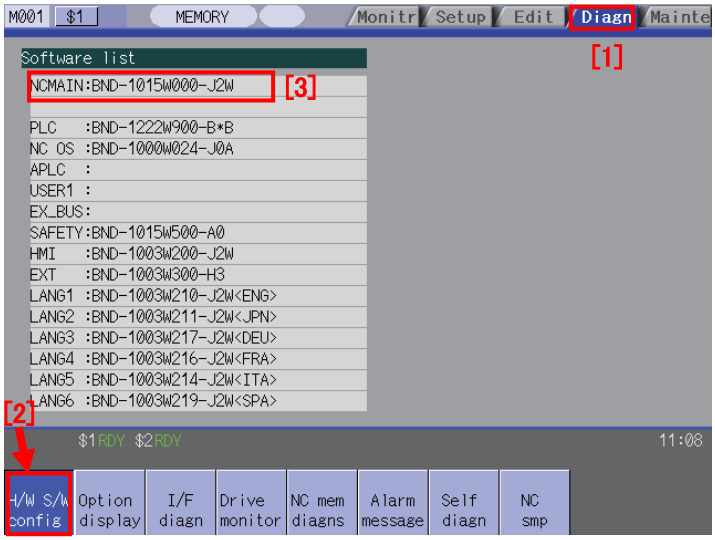

Figure 4. Software Configuration screen (M700V/M70V/E70 Series)

For NC Trainer2 and NC Trainer2 plus, check the “System Number” by following steps.

1) Start the program.
2) Click "Help" (see [1] in Figure 5) - "Version Information" (see [2] in Figure 5) in the menu bar to display the Version Information screen and check the “System Number” starting with BND (see [3] in Figure 5).

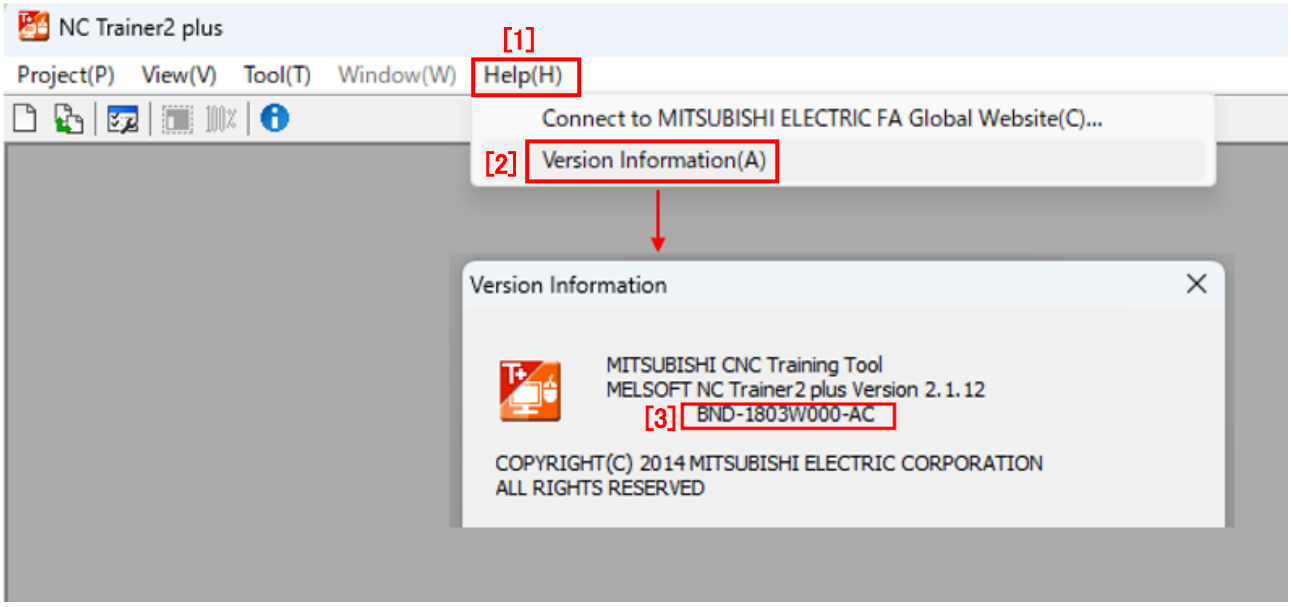

Figure 5. Version Information screen (NC Trainer2 and NC Trainer2 plus)

For details, please refer to the following instruction manuals.

Series	Instruction Manual	Reference
M800V/M80V Series	M800V/M80V Series Instruction Manual	https://www.mitsubishielectric.com/fa/download/index.html
M800/M80/E80 Series	M800/M80/E80 Series Instruction Manual	
C80 Series	C80 Series Instruction Manual	
M700V/M70V/E70 Series	M700V/M70V/E70 Series Instruction Manual	
Software Tools	NC Trainer2/NC Trainer2 plus Instruction Manual	

Description

A denial of service (DoS) vulnerability due to Improper Validation of Specified Index, Position, or Offset in Input (CWE-1285)[2] exists in the affected products.

Impact

A remote attacker may be able to cause an out-of-bounds memory read by sending specially crafted packets to TCP port 683. This may result in a denial of service (DoS) condition, causing the products to enter emergency shutdown. A system reset is required for recovery.

Countermeasures for Customers

Please refer to the table in "Countermeasures for Products" to determine whether a fixed version is available for your product.

<Customers using products with a fixed version available>

Please apply the fixed version. For instructions on how to apply it, please consult your Mitsubishi Electric representative.

<Customers using products without a fixed version available>

Please take the mitigation measures or workarounds described below.

Countermeasures for Products

The series, product names, system numbers and versions in which the vulnerability has been fixed are as follows.

Series	Product Name	System Number (**=Version)	Version
M800V/M80V Series	M800VW	BND-2051W000-**	BC or later
	M800VS	BND-2052W000-**	
	M80V	BND-2053W000-**	
	M80VW	BND-2054W000-**	
M800/M80/E80 Series	M800W	BND-2005W000-**	FN or later
	M800S	BND-2006W000-**	
	M80	BND-2007W000-**	
	M80W	BND-2008W000-**	
	E80	BND-2009W000-**	

Mitigations/Workarounds

Mitsubishi Electric recommends that customers take the following mitigating measures to minimize the risk of exploiting this vulnerability.

- Use a firewall, virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Use IP filter function*1 to block access from untrusted hosts.

  *1: IP filter function is available for M800V/M80V Series and M800/M80/E80 Series.
  For details about the IP filter function, please refer to the following manual for each product.
  M800V/M80V Series Instruction Manual "16. Appendix 3 IP Address Filter Setting Function"
  M800/M80/E80 Series Instruction Manual "15. Appendix 2 IP Address Filter Setting Function"
- Restrict physical access to the affected products and to all computers and network devices to which the products are connected.
- Install anti-virus software on your computers that have access to the affected products.

Contact information

Please contact your local Mitsubishi Electric representative.

〈Inquiries | MITSUBISHI ELECTRIC FA〉

https://www.mitsubishielectric.com/fa/service-support/index.html

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