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

Release date: October 17, 2024
Mitsubishi Electric Corporation

Overview

A denial of service (DoS) vulnerability exists in Numerical Control Systems (CNC). A malicious unauthenticated remote attacker may cause a denial of service (DoS) condition in the affected product by sending specially crafted packets to TCP port 683. (CVE-2024-7316)

The product models and system versions affected by this vulnerability are listed below.

CVSS[1]

CVE-2024-7316 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	System Number (**=Version)	Version
M800V/M80V Series	M800VW	BND-2051W000-**	All versions
	M800VS	BND-2052W000-**	
	M80V	BND-2053W000-**	
	M80VW	BND-2054W000-**	
M800/M80/E80 Series	M800W	BND-2005W000-**	
	M800S	BND-2006W000-**	
	M80	BND-2007W000-**	
	M80W	BND-2008W000-**	
	E80	BND-2009W000-**	
C80 Series	C80	BND-2036W000-**	
M700V/M70V/E70 Series	M750VW	BND-1015W002-**	
	M730VW/M720VW	BND-1015W000-**	
	M750VS	BND-1012W002-**	
	M730VS /M720VS	BND-1012W000-**	
	M70V	BND-1018W000-**	
	E70	BND-1022W000-**	
Software Tools	NC Trainer2	BND-1802W000-**	
	NC Trainer2 plus	BND-1803W000-**	

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

1) Display "Diagnostics" screen on the display unit of CNC, select "Config" menu and display "S/W Configuration" screen.
2) Confirm "System Number" displayed in "NCMAIN1" item on "S/W Configuration" screen.

For NC Trainer2 and NC Trainer2 plus, check the "System Number" by following steps.
1) Start the program.
2) Click "Help" - "Version Information" in the menu bar to display the version information screen and check the system number starting with BND.

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 exists in the affected products due to improper validation of specified quantity in input (CWE-1284)[2].

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

[2] https://cwe.mitre.org/data/definitions/1284.html

Impact

A malicious unauthenticated remote attacker may cause a denial of service (DoS) condition on the affected product by sending specially crafted packets to TCP port 683, causing an emergency stop.
In addition, system reset is required for recovery.

Countermeasures

Please use mitigations and workarounds. Fixed versions will be released at a later date.

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.
- Install anti-virus software on your PC that can access the product.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Restrict physical access to the affected product and the LAN to which the product is connected.
- 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"

Contact information

Please contact your local Mitsubishi Electric representative.

〈Inquiries｜MITSUBISHI ELECTRIC FA〉

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