

Denial of Service (DoS) and Malicious Code Execution Vulnerability in MITSUBISHI CNC Series

Release date: July 27, 2023
Last Update date: November 21, 2023
Mitsubishi Electric Corporation

■ Overview

Denial of Service (DoS) and Malicious Code Execution vulnerability exists in MITSUBISHI CNC series. A malicious remote attacker may cause DoS condition and execute malicious code on the product by sending specially crafted packets. (CVE-2023-3346)
The product models and system versions affected by this vulnerability are listed below.

■ CVSS¹

CVE-2023-3346 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Base Score:9.8

■ Affected products

The following products, System Number and Versions are affected:

Series	Product	System Number (**=Version)	Version
M800V/M80V Series	M800VW	BND-2051W000-**-**	A8 and prior
	M800VS	BND-2052W000-**-**	
	M80V	BND-2053W000-**-**	
	M80VW	BND-2054W000-**-**	
M800/M80/E80 Series	M800W	BND-2005W000-**-**	FB and prior
	M800S	BND-2006W000-**-**	
	M80	BND-2007W000-**-**	
	M80W	BND-2008W000-**-**	
	E80	BND-2009W000-**-**	
C80	C80	BND-2036W000-**-**	All versions
M700V/M70V/E70 Series	M750VW	BND-1015W002-**-**	LF and prior
	M730VW/M720VW	BND-1015W000-**-**	
	M750VS	BND-1012W002-**-**	
	M730VS/M720VS	BND-1012W000-**-**	
	M70V	BND-1018W000-**-**	
	E70	BND-1022W000-**-**	
IoT Unit	Remote Service Gateway Unit	BND-2041W001-**-**	All versions
	Data Acquisition Unit	BND-2041W002-**-**	

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 IoT Unit, open the web configuration tool from a web browser on your PC and check the "S/W Version" displayed on the tool's screen.

■ Description

Denial of service (DoS) and malicious code execution vulnerability exists in the product due to "Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')"(CWE-120)².

■ Impact

A malicious remote attacker may cause DoS condition and execute malicious code on the product by sending specially crafted packets. In addition, system reset is required for recovery.

¹ <https://www.first.org/cvss/v3.1/specification-document>

² <https://cwe.mitre.org/data/definitions/120.html>

■ Countermeasures

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

<Series, system number and version>

Series	Product	System Number (**=Version)	Version
M800V/M80V Series	M800VW	BND-2051W000-**	A9 or later
	M800VS	BND-2052W000-**	
	M80V	BND-2053W000-**	
	M80VW	BND-2054W000-**	
M800/M80/E80 Series	M800W	BND-2005W000-**	FC or later
	M800S	BND-2006W000-**	
	M80	BND-2007W000-**	
	M80W	BND-2008W000-**	
	E80	BND-2009W000-**	
M700V/M70V/E70 Series	M750VW	BND-1015W002-**	LG or later
	M730VW/M720VW	BND-1015W000-**	
	M750VS	BND-1012W002-**	
	M730VS/M720VS	BND-1012W000-**	
	M70V	BND-1018W000-**	
	E70	BND-1022W000-**	

<How to apply fixed version>

Please contact your local Mitsubishi Electric representative for information on how to apply the fixed version.

■ Mitigations/Workarounds

For customers who cannot update their systems immediately, Mitsubishi Electric recommends taking the mitigations listed below to minimize the risk of exploitation of this vulnerability.

- Use a firewall or 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.

■ Acknowledgement

Mitsubishi Electric would like to thank 01dGu0 of ZHEJIANG QIAN INFORMATION&TECHNOLOGY CO., LTD. who reported this vulnerability.

■ Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>

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

■ Update history

November 21, 2023

Added products that have been fixed to "Countermeasures".

M800VW, M800VS, M80V, M80VW, M750VW, M730VW/M720VW, M750VS, M730VS/M720VS, M70V, E70

October 31, 2023

Corrected Product and System Number of "Affected products".

Corrected System Number of M730VS

Deleted M750VS 15-type and M730VS/M720VS 15-type

Added products that have been fixed to "Countermeasures".

M800W, M800S, M80, M80W, E80

August 3, 2023

Corrected Product and System Number of "Affected products".

M730VW/M720VW, M720VS

Added Product and System Number that have been fixed to "Affected products".

M750VW, M750VS, M730VS, M750VS 15-type, M730VS/M720VS 15-type