

Remote Code Execution Vulnerability due to Microsoft Message Queuing in Electrical Discharge Machines

Release date: February 20, 2024

Last updated: April 23, 2024

Mitsubishi Electric Corporation

Overview

Remote code execution vulnerability due to Microsoft Message Queuing service on Microsoft Windows exists in Electrical discharge machines. A malicious remote attacker may execute malicious code on the product by sending specially crafted packets. As a result, the attacker may disclose, tamper with, destroy or delete information in the products, or cause a denial-of-service (DoS) condition on the products. System restart or system reinstallation are required for recovery. (CVE-2023-21554)

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

CVSS¹

CVE-2023-21554 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.

Refer to the following paragraphs in the instruction manual for methods for checking System Number, Versions and whether a Special Modification Patch is installed. (“e-manual” button at the bottom right of the operation screen on Electrical discharge machines enables you to refer to the instruction manual.)

• Instruction Manual for Wire-cut EDM:

VI. NC OPERATION DISPLAY SCREEN – 3. Initial setting – 3.3 SYSTEM UPDATE – 3.3.3 VERSION

• Instruction Manual for Sinker EDM

V. NC OPERATION DISPLAY SCREEN – 3. Initial setting – 3.3 SYSTEM UPDATE – 3.3.2 VERSION

Series	Product type name	System Number	Version
Wire-cut EDM MV Series	MV1200S	D-CUBES Series Standard system BRD-B60W000	Standard system versions B13 and prior, without Special Modification Patch BRD- C62W003-A0 installed Special system all versions
	MV2400S		
	MV4800S		
	MV1200R	D-CUBES Series Special system BRD-B63W000 to W036	
	MV2400R		
MV4800R			
Wire-cut EDM MP Series	MP1200		
	MP2400		
	MP4800		
Wire-cut EDM MX Series	MX900		
	MX2400		
Sinker EDM SV-P Series	SV8P	D-CUBES Series Standard system BRD-M60W000	Standard system versions A12 and prior, without Special Modification Patch BRD- C62W003-A0 installed
	SV12P		
Sinker EDM SG Series	SG8	D-CUBES Series Special system BRD-M63W000 to W022	Special system all versions
	SG12		
	SG28		

Description

Remote code execution vulnerability due to Microsoft Message Queuing service on Microsoft Windows exists in Electrical discharge machines. (CVE-2023-21554)

Impact

A malicious remote attacker may execute malicious code on the product by sending specially crafted packets. As a result, the attacker may disclose, tamper with, destroy or delete information in the products, or cause a denial-of-service (DoS) condition on the products. System restart or system reinstallation are required for recovery.

Countermeasures

Please install the Special Modification Patch BRD-C62W003-A0 on your system.

For information about how to install the update program, please contact your local service center.

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

Mitigations / Workarounds

Mitsubishi Electric recommends taking the mitigations listed below to minimize the risk of exploitation of 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.
- Restrict physical access to the affected products and to personal computers and network devices that can communicate with them.
- Install anti-virus software on personal computers that can communicate with the affected products.

Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>

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

Update history

April 23, 2024

Added Special Modification Patch information to “Countermeasures”.