مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Mitsubishi Electric Electrical Discharge Machines

Tracking #:432315792

Date:26-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Mitsubishi Electric released patches to address a critical vulnerability in electrical discharge machines.

TECHNICAL DETAILS:

A Remote code execution vulnerability exists in electrical discharge machines due to Microsoft Message Queuing service . 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

Vulnerability Details:

- **CVE ID:** CVE-2023-21554
- **CVSS 3.1 Score:** Base Score 9.8

Affected Products:

- Refer Mitsubishi Advisory

Mitigation:

- Mitsubishi Electric recommends that users install the Special Modification Patch BRD-C62W003-A0 on their system.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the patches released for affected products.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-022_en.pdf