Attackers Can Trigger Lockouts on Mitsubishi MELSEC iQ-F Devices

TL;DR

A remotely exploitable Denial-of-Service (DoS) vulnerability impacts Mitsubishi Electric MELSEC iQ-F devices due to an overly strict account lockout mechanism.

Attackers can temporarily lock out legitimate users. Mitsubishi will not release a patch, so immediate mitigations are the best course of action.

Overview

Mitsubishi Electric MELSEC iQ-F Series controllers have a built-in security feature designed to lock user accounts after too many incorrect login attempts. However, this feature is overly strict (CVE-2025-5241) and can be abused by attackers to intentionally cause denial-of-service conditions. Attackers can simply enter incorrect passwords repeatedly, locking out legitimate users and potentially disrupting critical manufacturing operations.

The issue affects numerous MELSEC iQ-F models, including FX5U, FX5UC, FX5UJ, FX5S, and FX5-CCLGN-MS series controllers.

CVE-2025-5241 stems from an excessively aggressive account-lockout mechanism (CWE-645). Because the attack method is straightforward, the risk of disruption is high even though the vulnerability itself has a moderate CVSS score of 6.9. Downtime in manufacturing is expensive and disruptive, and since Mitsubishi isn't providing a patch, teams should apply the recommended mitigations as soon as possible.

Aspire Protects

- Block external connections using firewalls or VPNs.
- Enable IP filtering to deny access from unknown or suspicious sources.
- Physically secure the controllers and connected networks.
- Review Mitsubishi's detailed IP filtering guidance here.

TTPs to Watch

Impact

- Service Stop [T1489] – Watch for repeated login attempts triggering lockout

IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations across the manufacturing sector are impacted by this vulnerability.

- Critical Manufacturing (especially facilities dependent on continuous device availability.)

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Denial-of-Service Vulnerability in MELSEC iQ-F Series

Mitsubishi Electric MELSEC iQ-F Series | CISA