1 Coordinated Vulnerability Disclosure Policy

Document Version: 1.0
Date: 2025-08-26
Product: EMF Device (EMF-AA01GLB-A)
Manufacturer: E M Fluids Inc.

1.1 Overview

This Coordinated Vulnerability Disclosure (CVD) Policy establishes the framework for reporting, assessing, and disclosing security vulnerabilities in EMF Device products and services. This policy is required by the Cyber Resilience Act (CRA) Annex I, Part II, point (5).

1.2 Policy Statement

E M Fluids Inc. is committed to maintaining the security of our products and services. We encourage security researchers, customers, and other stakeholders to report potential vulnerabilities to us so we can address them promptly and protect our users.

1.3 Scope

This policy applies to:

- EMF Device hardware (EMF-AA01GLB-A)
- Device firmware and software (PCM firmware, STM firmware)
- Cloud infrastructure
- Mobile application (EMFConnect)
- All associated services and APIs
- Communication protocols (LTE, BLE, UART)

1.4 System Architecture

The EMF Device system consists of: - **Cloud (AWS Stack)**: Central management and data processing - **Mobile App (EMFConnect)**: Local device management via BLE - **EMF Device (Firmware)**: Main device control and communication - **STM Device (Firmware)**: Hardware interface and control - **Communication Paths**: - Cloud EMF Device via Internet (LTE) - Cloud Mobile App EMF Device via BLE - EMF Device STM Device

1.5 Vulnerability Reporting

1.5.1 How to Report

Primary Contact: support@emfluids.com **Response Time**: Initial acknowledgment within 48 hours

1.5.2 Information to Include

When reporting a vulnerability, please provide: 1. **Description**: Clear description of the vulnerability 2. **Steps to Reproduce**: Detailed steps to reproduce the issue 3. **Impact Assessment**: Potential impact of the vulnerability 4. **Affected Components**: Specific products, versions, or services affected 5. **Proof of Concept**: If available, proof of concept code or demonstration 6. **Contact Information**: Your preferred contact method for follow-up

1.5.3 What We Consider a Vulnerability

- Security flaws that could lead to unauthorized access
- Data exposure or leakage

- Authentication or authorization bypasses
- Code injection vulnerabilities
- Cryptographic weaknesses
- Denial of service vulnerabilities
- Physical security issues affecting digital components
- Firmware tampering or modification
- Configuration tampering
- Update distribution vulnerabilities

1.6 Response Process

1.6.1 Phase 1: Acknowledgment (48 hours)

- Confirm receipt of vulnerability report
- Assign internal tracking number
- Provide initial assessment timeline

1.6.2 Phase 2: Assessment (5-10 business days)

- Technical analysis of the reported vulnerability
- Risk assessment and severity classification
- Determination of affected products and versions
- Development of remediation plan

1.6.3 Phase 3: Remediation (Timeline varies by severity)

- Development and testing of security fixes
- Creation of security advisory
- Coordination with stakeholders
- Preparation for public disclosure

1.6.4 Phase 4: Disclosure (Coordinated timeline)

- Public disclosure of vulnerability
- Release of security updates
- Communication to affected users
- Publication of security advisory

1.7 Severity Classification

1.7.1 Critical

- **Timeline**: Immediate response required
- **Examples**: Remote code execution, authentication bypass, firmware tampering
- **Response**: 48-hour acknowledgment, 10-day assessment

1.7.2 High

- **Timeline**: High priority response
- **Examples**: Data exposure, privilege escalation, update tampering
- **Response**: 72-hour acknowledgment, 14-day assessment

1.7.3 Medium

- **Timeline**: Standard response
- **Examples**: Information disclosure, limited DoS, configuration tampering
- **Response**: 1-week acknowledgment, 30-day assessment

1.7.4 Low

- **Timeline**: Lower priority response
- **Examples**: Minor information disclosure, UI issues, debug information exposure
- **Response**: 2-week acknowledgment, 60-day assessment

1.8 Disclosure Timeline

1.8.1 Standard Disclosure

- **Initial Disclosure**: Within 90 days of confirmed vulnerability
- **Public Advisory**: Within 30 days of fix availability
- **Coordinated Disclosure**: When possible, coordinate with other affected parties

1.8.2 Extended Timeline

- **Complex Vulnerabilities**: May require extended timeline
- **Coordinated Response**: When multiple vendors are affected
- **Regulatory Requirements**: Compliance with applicable regulations

1.9 Security Advisory Format

Our security advisories will include: 1. **Vulnerability Description**: Clear explanation of the issue 2. **Affected Products**: Specific products and versions 3. **Severity Rating**: Our classification 4. **Impact Assessment**: Potential consequences 5. **Remediation Steps**: How to fix or mitigate 6. **Timeline**: When fixes will be available 7. **Contact Information**: How to get additional help

1.10 Legal Considerations

1.10.1 Safe Harbor

- **Good Faith Research**: We will not pursue legal action against researchers who follow this policy
- **Scope Limitations**: Research must be within the scope defined above
- **Responsible Disclosure**: Researchers must not exploit vulnerabilities beyond what's necessary to demonstrate the issue

1.10.2 Exclusions

- **Social Engineering**: Phishing, pretexting, or similar tactics
- **Physical Attacks**: Physical access to devices or facilities
- **Denial of Service**: Testing that could impact service availability
- **Data Exfiltration**: Accessing or extracting user data
- **Operational Interference**: Testing that could affect device operations

1.11 Current Security Posture

Based on our threat model analysis, the following security controls are in place:

1.11.1 Authentication & Authorization

- Certificates for device authentication
- Certified 3rd party authentication service with MFA
- Role-based access control (RBAC)

1.11.2 Data Protection

- TLS/HTTPS encryption for all communications
- Data encryption at rest
- Data minimization practices

1.11.3 Integrity Protection

- Secure bootloader with firmware signing
- Signed firmware updates via HTTPS
- Data signing and integrity checks

1.11.4 Availability Protection

- BLE fallback for offline operation
- DDoS protection
- Rate limiting and resource protection

1.12 Contact Information

Support Team: support@emfluids.com

Mailing Address:
EM Fluids Inc. 87 Bentley Avenue, Nepean Ontario K2E 6T7 Canada

1.13 Policy Updates

This policy will be reviewed and updated annually or as needed to reflect: - Changes in regulatory requirements - Industry best practices - Organizational changes - Lessons learned from vulnerability handling

1.14 Compliance

This policy is designed to comply with: - Cyber Resilience Act (CRA) Annex I, Part II, point (5) - Industry best practices for coordinated vulnerability disclosure - ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure

---

Document Version: 1.0
Date: 2025-08-26