

Responsible Disclosure Policy

At MCL, the security of our software products and services is a top priority. Despite rigorous quality assurance, vulnerabilities can occasionally occur. If you believe you have discovered a security flaw in any MCL-owned software or source code, we ask you to report it to us privately. We appreciate your collaboration in helping us better protect our customers and systems.

Disclosure Process

Please do not report security vulnerabilities through public channels. Instead, submit your findings directly to the MCL Cyber Security Incident Response Team at security@mcl-technologies.com.

We prefer all communications to be in **English**. To help us triage and resolve the issue quickly, please provide as much of the following information as possible:

- **Issue Type:** (e.g., SQL injection, XSS, buffer overflow)
- **Affected Paths:** Full paths of the source files related to the issue
- **Code Location:** The affected source code location (tag, branch, commit hash, or direct URL)
- **Configuration:** Any specific system configurations required to reproduce the flaw
- **Reproduction Steps:** Clear, step-by-step instructions to reproduce the issue
- **Impact:** A description of the impact and how an attacker could exploit it

Communication Timeline

We will acknowledge receipt of your report as soon as possible and provide regular progress updates. If you have questions about the status of your report, or if you do not receive a timely response, please follow up with us via email to ensure your original message was received.

Rules of Engagement

To responsibly disclose a vulnerability, you must adhere to the following rules:

- **No Public Disclosure:** Do not disclose the vulnerability publicly or to any third party until we have resolved the issue.
- **Data Minimization:** Do not exploit the vulnerability beyond what is strictly necessary to demonstrate it. Do not unnecessarily copy, delete, adapt, view, or download data.
- **Data Destruction:** Immediately erase all exfiltrated or obtained data once the issue has been reported to MCL.
- **System Integrity:** Avoid any actions that could impact the availability, performance, confidentiality, or integrity of our systems and data.

Strictly Prohibited Actions:

- Deploying malware (viruses, worms, Trojan horses, etc.)
- Modifying, deleting, or altering data or configurations within a system
- Maintaining persistent access or sharing access with third parties
- Executing automated scanning tools or brute-force attack
- Launching Denial of Service (DoS/DDoS) attacks
- Utilizing social engineering tactics (phishing, vishing, spam, etc.)
- Attempting physical security attacks on our facilities

Out of Scope (What NOT to Report)

The following issues are considered out of scope and should not be reported unless they directly lead to a critical exploit (such as an account takeover):

- Cookies missing HttpOnly or Secure flags
- Missing HTTP security headers
- Software version disclosure or banner identification
- Missing SSL/TLS configuration best practices
- Email configuration issues (including missing SPF, DKIM, DMARC, or MTA-STS records)
- Missing rate limits (unless leading to account takeover)

Publication and Attribution

If you wish to publish information about the vulnerability after it has been remediated, you must **notify us at least one month prior to publication** to give us an opportunity to respond. You may only identify MCL in your publication if you have received our explicit written approval.

Policy Terms

MCL reserves the right to modify or terminate this policy at any time. If you are unsure whether an action is permitted under this policy, please contact us at **security@mcl-technologies.com** to request explicit permission before proceeding.

Thank you for your efforts and for working with us to keep our software secure.