Vulnerability Management Policy

Organization: Caliber Technologies Inc. (Calimatic Mail) **Document Version:** 1.0 **Effective Date:** February 14, 2026 **Last Reviewed:** February 14, 2026 **Classification:** Confidential

---

1. Purpose

This policy establishes procedures for identifying, assessing, prioritizing, and remediating security vulnerabilities across the Calimatic Mail platform.

2. Scope

This policy covers:

- Application dependencies (npm packages)
- Application source code
- Infrastructure components (Docker images, Traefik, PostgreSQL, Redis)
- Third-party integrations (Zoom, Google OAuth)

3. Vulnerability Identification

3.1 Dependency Scanning

- **Tool:** `npm audit` against the GitHub Advisory Database.
- **Frequency:** On every build and at minimum monthly.
- **Scope:** All packages in the monorepo (API, webmail, admin, superadmin, marketing).

3.2 Code Review

- All code changes undergo peer review with attention to OWASP Top 10 risks.
- Security-sensitive changes (auth, token handling, integrations) receive dedicated security review.

3.3 Security Advisories

- The engineering team monitors security advisories for:
  - Node.js runtime
  - Fastify framework
  - Next.js framework
  - PostgreSQL
  - Redis
  - Docker base images
  - Zoom and Google API changes

3.4 Runtime Monitoring

- Application logs are monitored for anomalous patterns (auth failures, rate limit hits, error spikes).
- Prometheus/Grafana dashboards provide real-time visibility into system health.

4. Vulnerability Assessment

4.1 Severity Classification

Vulnerabilities are classified using the following severity levels, aligned with CVSS scoring:

Severity	CVSS Score	Description
Critical	9.0 - 10.0	Actively exploitable, remote code execution, data breach risk
High	7.0 - 8.9	Significant impact, exploitable with moderate effort

Moderate	4.0 - 6.9	Limited impact, requires specific conditions
Low	0.1 - 3.9	Minimal impact, informational

4.2 Impact Assessment

Each vulnerability is assessed for:

- **Production exposure:** Is the affected component present in production images?
- **Exploitability:** Can the vulnerability be triggered in the application's specific usage pattern?
- **Mitigating controls:** Are there existing controls (rate limiting, input validation, network isolation) that reduce risk?
- **Data sensitivity:** Could exploitation expose user data, tokens, or credentials?

4.3 Risk Rating

The combination of severity and impact assessment produces a risk rating:

- **Critical Risk:** Actively exploitable in production, immediate response required
- **High Risk:** Exploitable in production with reasonable effort
- **Medium Risk:** Limited production exposure or strong mitigating controls
- **Low Risk:** Development-only dependency or theoretical risk only

5. Remediation

5.1 Response Timeframes

Risk Rating	Response Timeframe	Action
Critical	24 hours	Emergency patch, potential service maintenance window
High	72 hours	Patch applied and deployed
Medium	14 days	Patch applied in next scheduled release
Low	30 days	Tracked and resolved in next maintenance cycle

5.2 Remediation Actions

1. **Patch:** Apply the vendor-provided fix via dependency update.
2. **Workaround:** If no patch is available, implement a compensating control.
3. **Mitigate:** If the vulnerability cannot be immediately resolved, document mitigating controls and track for resolution.
4. **Accept:** For vulnerabilities with no production impact (e.g., dev-only dependencies), document the risk acceptance with justification.

5.3 Verification

- After applying a fix, re-run `npm audit` to confirm the vulnerability is resolved.
- Test the affected functionality to ensure no regression.
- Update the SAST report with remediation results.

6. Reporting

6.1 SAST Reports

- SAST reports are generated after each audit cycle.
- Reports include: total vulnerabilities, severity breakdown, remediation actions taken, and remaining items with risk assessments.
- Reports are stored in `/docs/policies/SAST-Report.md`.

6.2 Tracking

- Open vulnerabilities are tracked with severity, affected package, remediation plan, and target date.
- Resolved vulnerabilities are documented with the fix version and verification date.

7. Responsible Disclosure

If a security researcher discovers a vulnerability in Calimatic Mail:

- Report to: security@calimatic.app
- We acknowledge receipt within 48 hours.
- We provide an initial assessment within 7 days.
- We coordinate disclosure timelines with the reporter.

8. Review Cycle

This policy is reviewed quarterly and updated when:

- New scanning tools or processes are adopted
- Severity thresholds are adjusted
- Significant infrastructure changes occur

Approved by: Engineering Team, Caliber Technologies Inc. **Contact:** security@calimatic.app