

Vulnerability and Patch Management Procedure

Owner	Andrew Smith, Security Owner
Version	1.1, effective October 19, 2026
Part of	Swapt Information Security Policy

1. Scope

This procedure covers the Swapt application code, its third-party dependencies (npm packages), container base images, cloud configuration and company endpoints.

2. Identifying vulnerabilities

Source	How it is used
<code>pnpm audit</code>	Checks every dependency against the npm advisory database; run before each release and in the monthly maintenance pass
Code review	Every change is reviewed in a pull request before release, including automated review that checks for security issues such as injection, missing authorization checks and secrets in code
Provider advisories	Security bulletins from Google Cloud, AWS, Cloudflare, Node.js and AdonisJS are followed
Monitoring	Unusual errors and failures in Sentry and the platform logs are investigated as possible exploitation
External reports	Researchers, partners and customers can report issues to andrew@swaptqr.com

3. Assessing vulnerabilities

Each finding is logged and rated using its CVSS score, adjusted for how it affects Swapt: whether the vulnerable code is reachable, whether it is exposed to the internet, and what data is at risk.

Rating	Typical CVSS	Fix target
Critical	9.0 to 10.0, or actively exploited	7 days, or immediate mitigation
High	7.0 to 8.9	14 days
Medium	4.0 to 6.9	30 days

Rating	Typical CVSS	Fix target
Low	Below 4.0	90 days, or the next scheduled update

4. Fixing vulnerabilities and patching

- Fixes are made as normal pull requests: reviewed, tested by the automated test and type-check pipeline, and deployed through the standard release process.
- Dependencies are upgraded to a fixed version. Where no fix exists yet, the vulnerability is mitigated by removing or disabling the affected code path, adding input validation, or blocking it at the edge. The finding stays open until a fix is released.
- **Infrastructure patching.** Google Cloud patches the managed hosting platform and database, AWS and Cloudflare patch their edge services, and Swapt rebuilds its container image on each release, picking up updated base images.
- **Endpoint patching.** This follows the Endpoint Protection Standard: critical macOS security updates within 7 days.
- A dependency maintenance pass runs at least once a month, even when there are no open alerts. The most recent pass, on October 13, 2026, upgraded every dependency with a known vulnerability.

5. Recent security fixes

In October 2026 we tightened authorization on unauthenticated endpoints, made sign-in answers identical for unknown accounts, made webhook signature checks mandatory in every environment, stopped partner API keys from appearing in logs, and moved super-admin sign-in to Google accounts with 2-Step Verification.

6. Tracking and reporting

- Open vulnerabilities are tracked in the issue tracker until they are closed.
- Every month, the Security Owner reviews open findings against the fix targets. Overdue items are escalated and recorded in the security log.
- Exceptions (accepted risk) need the Security Owner's written approval, with a reason, compensating controls and a review date.
- A vulnerability that has been exploited is handled as an incident under the Incident Response Plan.