

# Dependabot Alerts & Updates — Quick Cheatsheet

Enable, configure, and triage GitHub dependency updates with confidence.

Scope: GitHub repos  
Audience: Dev, Sec, Maintainers

**Key defaults:** *Public* repos have alerts on by default. *Private* repos require enabling in Settings. Viewing alerts typically requires `read+` access; enabling/managing may require `admin` depending on org policy.

## 1 Enable & Visibility

- Repo → Settings → Code security & analysis → toggle Dependabot alerts.
- Who can view:** anyone with `read+` (and everyone for public repos).
- Who can enable/manage:** usually `admin/maintain`; org policies may restrict repo-level toggles.

### Roles (repo level)

|               | Read | Triage | Write | Maint. | Admin |
|---------------|------|--------|-------|--------|-------|
| View alerts   | ✓    | ✓      | ✓     | ✓      | ✓     |
| Dismiss alert | ✗    | ✓      | ✓     | ✓      | ✓     |
| Merge PRs     | ✗    | ✓      | ✓     | ✓      | ✓     |
| Enable alerts | ✗    | ✗      | ✗     | ✓      | ✓     |

## Common Options

- `schedule.interval`: daily | weekly | monthly.
- `allow/ignore`: control which dependencies update.

## 2 Configuration Basics

File: `.github/dependabot.yml`

```
version: 2
updates:
  - package-ecosystem: "npm"      # npm, pip,
    ↳ gomod, maven, gradle, cargo, etc.
    directory: "/"                 # path to
    ↳ manifest(s)
    schedule:
      interval: "weekly"          # daily, weekly,
      ↳ monthly
    # groups:                      # optional:
    ↳ group related changes into one PR
    # minor-deps:
    #   patterns: ["*"]
    #   update-types: ["minor", "patch"]
  - package-ecosystem: "pip"
    directory: "/"
    schedule:
      interval: "weekly"
    ignore:                         # optional:
    ↳ ignore certain deps/versions
    - dependency-name: "example"
      versions: ["<1.2.3"]
```

- `open-pull-requests-limit`: cap concurrent update PRs.

## 3 Notifications & Automation

- Alerts:** GitHub notifications, email, or webhooks (e.g., Slack/Teams via your integration).
- PRs:** Auto-opened by Dependabot; configure required checks to ensure safe merges.
- Rules UI:** At org/repo scope you can define rules to auto-dismiss low-risk alerts or auto-open PRs by severity/ecosystem.

## 4 Triage & Remediation Flow

1. **Assess** severity, reachability, and exploitability.
2. **Decide** on *upgrade*, *pin*, *patch*, or *temporary dismiss*.
3. **Validate** with tests, SCA/SAST/DAST, and runtime checks.
4. **Merge** when CI passes; monitor post-deploy.

### Recommended Dismissal Reasons

- *Not affected* (unreachable code path).
- *Legacy/unmaintained* with compensating controls.
- *False positive* (erroneous advisory match).
- *Will fix* in planned upgrade window with ticket reference.

## 5 Best Practices

- Keep **interval** small for critical services; group minor/patch updates.
- Set **required checks** on Dependabot PRs (tests, build, security scans).
- Gate merges by **vuln severity** via branch protection or policy.
- Use **labels** and **codeowners** to route reviews quickly.
- Limit **concurrent PRs** to avoid queue congestion.

## 6 Sample Policies & Patterns

### Limit Concurrent PRs

```
version: 2
updates:
  - package-ecosystem: "npm"
    directory: "/"
    open-pull-requests-limit: 5
    schedule: { interval: "daily" }
```

### Group Minor/Patch Updates

```
updates:
  - package-ecosystem: "maven"
    directory: "/"
    schedule: { interval: "weekly" }
    groups:
      routine-minor-patch:
        patterns: ["*"]
        update-types: ["minor", "patch"]
```

### Ignore Specific Versions

```
updates:
  - package-ecosystem: "gomod"
    directory: "/"
    schedule: { interval: "weekly" }
    ignore:
      - dependency-name: "example.com/libfoo"
        versions: ["1.4.x", "<1.3.2"]
```

## 7 Quick Links

- **Repo Settings:** Code security & analysis → Dependabot alerts.
- **Config File:** `.github/dependabot.yml` at repo root.
- **Routing:** Labels + CODEOWNERS for fast PR assignment.

**Compile tip:** This document uses `minted` for syntax highlighting. Compile with `-shell-escape` enabled (e.g., `pdflatex -shell-escape`).