

RP - Correction des vulnérabilités

Runbook, Mai 2026. Workflow de correction des vulnérabilités de dépendances détectées par Dependabot.

Contexte

Les vulnérabilités sont détectées automatiquement par **Dependabot** et remontent chaque matin sur Slack. Ce document décrit la procédure complète de triage et correction, de l'alerte au merge.

Dependabot est configuré en **alerts only**, il ne crée pas de Pull Requests automatiques. Les corrections sont appliquées manuellement selon ce workflow.

Convention de nommage

Branche Git

Format : security/<package>-patch-dep<N>-<N>

Exemples :

security/phpspreadsheet-patch-dep5-9

security/axios-patch-dep10-22

Trello - Ticket de suivi

Etiquette: <projet>(RP) <prioritaire> <sécurité> et potentiellement <Non testable PO>.

Titre :

Format : Sécurité - Patch <package> <v.actuelle> → <v.cible> (dep N-N)

Exemples:

Sécurité - Patch phpspreadsheet 3.10.0 → 3.10.5 (dep #5-9) [1]

Sécurité - Patch axios 1.15.0 to 1.16.0 (dep 10-22) [1]

Description : liens vers les alertes de sécurité Dependabot

Exemple:

Fixes Dependabot alerts 19-22

19 - <https://github.com/re-connect/pro/security/dependabot/19>

20 - <https://github.com/re-connect/pro/security/dependabot/20>

21 - <https://github.com/re-connect/pro/security/dependabot/21>

22 - <https://github.com/re-connect/pro/security/dependabot/22>

Et bien sur, powers-up git pour les branches et les PRs.

Pull Request

Toujours 2 PRs, une vers `main` et une vers `dev` et attribuer au PRs le label `<security>` pour une meilleur lisibilité.

Titre :

Format: security(deps-<écosystème>): upgrade <package> <v.actuelle> to <v.cible>

Exemples:

security(deps-composer): upgrade phpspreadsheet 3.10.0 to 3.10.5

security(deps-yarn): upgrade axios 1.15.0 to 1.16.0

Description :

Exemple:

Fixes Dependabot alerts 10-22

22 - <https://github.com/re-connect/pro/security/dependabot/22>

21 - <https://github.com/re-connect/pro/security/dependabot/21>

20 - <https://github.com/re-connect/pro/security/dependabot/20>

19 - <https://github.com/re-connect/pro/security/dependabot/19>

- 18 - <https://github.com/re-connect/pro/security/dependabot/18>
- 17 - <https://github.com/re-connect/pro/security/dependabot/17>
- 16 - <https://github.com/re-connect/pro/security/dependabot/16>
- 15 - <https://github.com/re-connect/pro/security/dependabot/15>
- 14 - <https://github.com/re-connect/pro/security/dependabot/14>
- 13 - <https://github.com/re-connect/pro/security/dependabot/13>
- 12 - <https://github.com/re-connect/pro/security/dependabot/12>
- 11 - <https://github.com/re-connect/pro/security/dependabot/11>
- 10 - <https://github.com/re-connect/pro/security/dependabot/10>

Preview:

Fixes Dependabot alerts 10-22

- 22 - [Axios: CRLF Injection in multipart/form-data body via unsanitized blob.type in formDataToStream](#)
- 21 - [Axios: no_proxy bypass via IP alias allows SSRF](#)
- 20 - [Axios: unbounded recursion in toFormData causes DoS via deeply nested request data](#)
- 19 - [Axios' HTTP adapter-streamed uploads bypass maxBodyLength when maxRedirects: 0](#)
- 18 - [Axios: HTTP adapter streamed responses bypass maxContentLength](#)
- 17 - [Axios: Prototype Pollution Gadgets - Response Tampering, Data Exfiltration, and Request Hijacking](#)
- 16 - [Axios: Header Injection via Prototype Pollution](#)
- 15 - [Axios: XSRF Token Cross-Origin Leakage via Prototype Pollution Gadget in `withXSRFToken` Boolean ...](#)
- 14 - [Axios: Authentication Bypass via Prototype Pollution Gadget in `validateStatus` Merge Strategy](#)
- 13 - [Axios: Incomplete Fix for CVE-2025-62718 — NO_PROXY Protection Bypassed via RFC 1122 Loopback Sub...](#)
- 12 - [Axios: Invisible JSON Response Tampering via Prototype Pollution Gadget in `parseReviver`](#)
- 11 - [Axios has prototype pollution read-side gadgets in HTTP adapter that allow credential injection a...](#)
- 10 - [Axios: Null Byte Injection via Reverse-Encoding in AxiosURLSearchParams](#)



Procédure de triage

1. Évaluer le saut de version

Saut	Risque	Action
patch x.y.z	Nul	Update direct, pas de CHANGELOG à lire
minor x.Y.z	Faible	Lire le CHANGELOG, vérifier les releases notes
major X.y.z	Élevé	Lire le CHANGELOG, chercher une migration guide

2. Grouper les alertes

- Même package + même écosystème → **un seul batch**
- Écosystèmes différents (npm / composer) → **branches séparées**
- Breaking change dans le batch → **commit séparé** dans la même branche

Procédure de correction

Composer

Voir la procédure Composer

1. Vérifier la version installée :

```
composer show phpooffice/phpspreadsheet | grep versions
```

2. S'assurer que `composer.json` utilise `^` et non une version exacte :

```
"phpooffice/phpspreadsheet": "^3.10"
```

3. Mettre à jour le package :

```
composer update phpooffice/phpspreadsheet
```

4. Valider :

```
composer validate
```

```
composer audit
```

5. Commiter :

```
git add composer.json composer.lock
```

```
git commit -m "[ ] security(deps-composer): upgrade <package> <v.actuelle> to <v.cible>"
```

npm / Yarn

Voir la procédure Yarn

1. Vérifier la version installée :

```
yarn list axios
```

2. Mettre à jour le package :

```
yarn upgrade axios
```

3. Valider :

```
yarn audit
```

4. Commiter :

```
git add yarn.lock
```

```
git commit -m "[ ] security(deps-npm): upgrade <package> <v.actuelle> to <v.cible>"
```

Si `yarn upgrade` monte en minor au lieu du patch indiqué par Dependabot, vérifier que la minor n'introduit pas de breaking change avant de commiter.

Checklist avant merge

- CI verte
- `composer audit` ou `yarn audit` sans alerte bloquante
- 2 PRs ouvertes, `main` + `dev`
- Alertes Dependabot fermées après merge

Révision #8

Créé 7 mai 2026 10:57:35 par Romain Lacits

Mis à jour 5 juin 2026 13:20:52 par Romain Lacits