kevrea.

EXEMPLE FICTIF

ANALYSE DE SÉCURITÉ · DÉPENDANCES PHP

Dépendances PHP de

Exemple SARL

www.exemple.fr

Émis le 8 octobre 2026

CLIENT
Exemple SARL

ÉMIS LE
8 octobre 2026

PÉRIMÈTRE
41 paquets de production, 2 de développement

SOCLE
Drupal 10.2.3, Symfony 6.4.3

EN UN COUP D'ŒIL

NIVEAU DE RISQUE

Critique

6
paquets de production touchés sur 41

9
avis de sécurité en production

3
actions prioritaires (P1)

Ce que ce document est, et ce qu'il n'est pas

Chaque paquet du composer.lock a été rapproché des avis de sécurité publics à la date d'émission. Ce document dit quelles failles connues touchent le projet, ce qu'elles permettent et comment les corriger. Il ne remplace ni un test d'intrusion ni l'examen de l'usage réel de chaque paquet.

SYNTHÈSE

Synthèse pour la direction

L'essentiel, pour décider sans lire le détail.

NIVEAU DE RISQUE

Critique

Au moins une faille critique touche un paquet de production : à traiter sans attendre.

Recommandation

Traiter sans attendre les 3 actions prioritaires (P1), puis appliquer le reste du plan à la prochaine mise à jour planifiée. Relancer ensuite l'analyse pour contrôler que les avis ont disparu.

L'ESSENTIEL

- 41 paquets de production analysés (Drupal 10.2.3, Symfony 6.4.3). 6 sont concernés par au moins une faille connue, pour 9 avis de sécurité. Gravité : 2 critiques, 2 élevées, 4 moyennes, 1 faible.
- Les failles les plus sérieuses relèvent de : exécution de code à distance, requêtes forgées côté serveur (SSRF), fuite d'informations. Le détail de chaque faille, avec son impact, figure plus bas.
- Côté plan d'action : 4 corrections passent par une simple mise à jour compatible avec les contraintes actuelles ; 1 est bloquée par la contrainte d'un autre paquet ; 2 demandent une montée de version majeure.
- Drupal 10.2.3 : fin des correctifs de sécurité le 09/12/2026 ; la montée de version est à planifier dès maintenant.
- Le projet accepte encore PHP 8.1. Pour cette branche, plus aucun correctif de sécurité depuis le 31/12/2025 ; les failles découvertes ne seront plus corrigées. La version de PHP réellement utilisée par le serveur est à vérifier.
- 1 outil de développement est aussi concerné : sans effet en production s'il n'y est pas installé.
- 1 paquet de production est abandonné par ses auteurs : plus aucune correction à attendre, un remplacement est à prévoir.

Observations de Mathieu ROMEUF (exemple fictif)

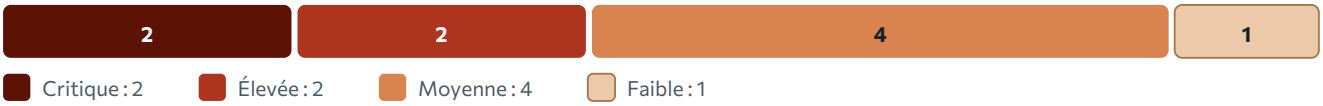
Le module d'export PDF n'est utilisé que dans l'administration du site : la faille d'exécution de code n'est exploitable que par un compte éditeur. Elle reste en priorité 1, car un compte éditeur peut être compromis. La montée vers Drupal 11 est à planifier avant la fin des correctifs de Drupal 10.

EXPOSITION

Où se situe le danger

Les failles des paquets de production, rangées par gravité puis par type de faille.

RÉPARTITION DES 9 AVIS PAR GRAVITÉ



Critique : 2 · Élevée : 2 · Moyenne : 4 · Faible : 1

CARTE DE CHALEUR : TYPE DE FAILLE × GRAVITÉ

	Critique	Élevée	Moyenne	Faible	Total
Exécution de code à distance	1				1
Requêtes forgées côté serveur (SSRF)	1				1
Injection de script (XSS)		1			1
Contournement des droits d'accès			1		1
Vérification ou chiffrement contournable			1		1
Fuite d'informations		1		1	2
Déni de service			1		1
Injection d'en-têtes ou de requêtes			1		1

La colonne donne la gravité, le chiffre le nombre de failles ; plus la case est soutenue, plus elle en compte. Le type est déduit de l'intitulé de chaque avis. Les failles des outils de développement (1) n'y figurent pas.

LES 41 PAQUETS DE PRODUCTION

Une case par paquet, colorée selon la faille la plus grave qui le touche.



Critique · Élevée · Moyenne · Faible · Aucune faille connue

PLAN D'ACTION

Quoi corriger, dans quel ordre

Une action par paquet touché. **P1** : à traiter sans attendre ; **P2** : à la prochaine mise à jour planifiée ; **P3** : lors de la maintenance courante. Pour chacune : la version à atteindre, l'ampleur de la mise à jour, et si les contraintes du projet la permettent.

GRAVITÉ ET EFFORT : LES GAINS RAPIDES SONT EN HAUT À GAUCHE

	Mise à jour simple	Contrainte à vérifier	Travail important	Sans correctif publié
CRITIQUE	1		2	
ÉLEVÉE	3			
MOYENNE	5	(6)	4	
FAIBLE	7			

Pastille pleine : paquet de production ; pastille cerclée : outil de développement. Les numéros renvoient aux actions ci-dessous.

P1 : à traiter sans attendre

1 `exemple/http-client` CRITIQUE

7.5.1 vers 7.8.0 · version mineure · Mise à jour compatible

Mettre à jour `exemple/http-client` vers la version 7.8.0 ou plus récente. Les contraintes actuelles du projet le permettent : une mise à jour Composer ciblée suffit.

COMMANDE INDICATIVE

```
composer update exemple/http-client --with-dependencies
```

2 `exemple/pdf-renderer` CRITIQUE

2.0.3 vers 3.0.1 · version majeure · Bloquée par une contrainte

Blocage : `drupal/core` exige `^2.0` › exclut `exemple/pdf-renderer 3.0.1`

La version corrigée 3.0.1 est exclue par la contrainte de `drupal/core` (`^2.0`). Il faut d'abord mettre à jour `drupal/core` vers une version qui accepte la correction. Il s'agit d'une montée de version majeure : prévoir la revue des changements incompatibles et des tests de non-régression. Attention : au moins un des avis n'a pas encore de correctif publié pour cette branche.

COMMANDE INDICATIVE

```
composer update drupal/core exemple/pdf-renderer --with-all-dependencies
```

3 `drupal/core` ÉLEVÉE

10.2.3 vers 10.2.6 · version corrective · Mise à jour compatible

Mettre à jour le cœur de Drupal vers la version 10.2.6 ou plus récente, en mettant à jour ensemble `drupal/core` et ses métapaquets (`drupal/core-recommended`, `drupal/core-composer-scaffold`), puis lancer les mises à jour de base de données (`drush updatedb`) et vider les caches.

COMMANDE INDICATIVE

```
composer update "drupal/core-*" --with-all-dependencies
```

P2 : à la prochaine mise à jour planifiée

4 `exemple/jwt` MOYENNE

5.5.1 vers 6.0.0 · version majeure · Contrainte à vérifier

Mettre à jour `exemple/jwt` vers la version 6.0.0 ou plus récente. Si Composer refuse, la contrainte déclarée dans le composer.json du projet est à élargir. Il s'agit d'une montée de version majeure : prévoir la revue des changements incompatibles et des tests de non-régression.

COMMANDE INDICATIVE

```
composer update exemple/jwt --with-dependencies
```

5 `exemple/psr7` MOYENNE

2.4.0 vers 2.4.5 · version corrective · Mise à jour compatible

Mettre à jour `exemple/psr7` vers la version 2.4.5 ou plus récente. Les contraintes actuelles du projet le permettent : une mise à jour Composer ciblée suffit.

COMMANDE INDICATIVE

```
composer update exemple/psr7 --with-dependencies
```

P3 : lors de la maintenance courante

6 `exemple/debug-bar` MOYENNE DÉVELOPPEMENT

1.2.0 vers 1.3.0 · version mineure · Contrainte à vérifier

Mettre à jour `exemple/debug-bar` vers la version 1.3.0 ou plus récente. Si Composer refuse, la contrainte déclarée dans le composer.json du projet est à élargir. Paquet de développement : sans effet en production s'il n'y est pas installé (`composer install --no-dev`).

COMMANDE INDICATIVE

```
composer update exemple/debug-bar --with-dependencies
```

7

exemple/yaml-parser FAIBLE

1.4.2 vers 1.4.9 · version corrective · Mise à jour compatible

Mettre à jour `exemple/yaml-parser` vers la version 1.4.9 ou plus récente. Les contraintes actuelles du projet le permettent : une mise à jour Composer ciblée suffit.

COMMANDE INDICATIVE

```
composer update exemple/yaml-parser --with-dependencies
```

Après chaque mise à jour : lancer les tests du projet, vérifier les fonctions qui utilisent le paquet, puis relancer l'analyse. Les avis corrigés ne doivent plus apparaître.

DÉTAIL

Détail des failles, paquet par paquet

Pour chaque avis : son identifiant public, sa gravité, ce qu'il permet à un attaquant, les versions touchées et la première version corrigée de la branche installée.

1 `exemple/http-client 7.5.1`

2 avis · pire gravité : critique · licence MIT

P1

Exigé par : `drupal/core` (`^7.5`).

CRITIQUE Requêtes forgées côté serveur (SSRF)

`CVE-2099-10002`

Ce que cela permet : Le serveur peut être utilisé pour envoyer des requêtes vers des services internes qui ne sont pas exposés sur Internet.

Intitulé de l'avis : Server-side request forgery through redirect handling

VERSIONS TOUCHÉES	CORRIGÉ EN	PUBLIÉ LE
`>=7.0.0,<7.8.0`	**7.8.0**	10/02/2025

ÉLEVÉE Fuite d'informations

`CVE-2099-10001`

Ce que cela permet : Des informations sensibles (identifiants, cookies, en-têtes d'autorisation, données internes) peuvent être exposées à un tiers.

Intitulé de l'avis : Failure to strip the Authorization header on HTTP downgrade

VERSIONS TOUCHÉES	CORRIGÉ EN	PUBLIÉ LE
`>=7.0.0,<7.5.4`	**7.5.4**	10/02/2025

2 `exemple/pdf-renderer 2.0.3`

2 avis · pire gravité : critique · licence LGPL-2.1

P1

Exigé par : `drupal/core` (`^2.0`).

CRITIQUE Exécution de code à distance

`CVE-2099-10004`

Ce que cela permet : Un attaquant peut faire exécuter ses propres instructions sur le serveur : prise de contrôle du site, vol ou destruction des données, rebond vers le reste du système d'information.

Intitulé de l'avis : Remote code execution via PHAR deserialization

VERSIONS TOUCHÉES	CORRIGÉ EN	PUBLIÉ LE
`>=2.0.0,<3.0.1`	**3.0.1**	10/02/2025

MOYENNE Déni de service

`CVE-2099-10005`

Ce que cela permet : Une requête malveillante peut ralentir fortement le site ou le rendre indisponible.

Intitulé de l'avis : Denial of service through nested CSS rules

VERSIONS TOUCHÉES	CORRIGÉ EN	PUBLIÉ LE
`<=2.0.4`	Aucun correctif publié pour cette branche	10/02/2025

3 drupal/core 10.2.3

2 avis · pire gravité : élevée · licence GPL-2.0-or-later

P1

Exigé par : `drupal/webform` (`^10`).

ÉLEVÉE **Injection de script (XSS)** SA-CORE-2099-002

Ce que cela permet : Un attaquant peut faire exécuter du script dans le navigateur des visiteurs ou des administrateurs : vol de session, actions en leur nom, défiguration des pages.

Intitulé de l'avis : Drupal core - Critical - Cross-site scripting - SA-CORE-2099-002

VERSIONS TOUCHÉES	CORRIGÉ EN	PUBLIÉ LE
`>=8.0.0,<10.2.5`	**10.2.5**	10/02/2025

MOYENNE **Contournement des droits d'accès** SA-CORE-2099-001

Ce que cela permet : Des personnes peuvent accéder à des contenus ou à des fonctions qui devraient leur être interdits, voire obtenir des droits d'administration.

Intitulé de l'avis : Drupal core - Moderately critical - Access bypass - SA-CORE-2099-001

VERSIONS TOUCHÉES	CORRIGÉ EN	PUBLIÉ LE
`>=10.0.0,<10.2.6|>=10.3.0,<10.3.1`	**10.2.6**	10/02/2025

4 exemple/jwt 5.5.1

1 avis · pire gravité : moyenne · licence BSD-3-Clause

P2

Dépendance directe probable du projet (aucun autre paquet ne l'exige).

MOYENNE **Vérification ou chiffrement contournable** CVE-2099-10006

Ce que cela permet : Un contrôle de sécurité (signature, jeton, certificat, mot de passe) peut être contourné ou affaibli : usurpation d'identité ou falsification possibles.

Intitulé de l'avis : Algorithm confusion allows signature verification bypass

VERSIONS TOUCHÉES	CORRIGÉ EN	PUBLIÉ LE
`>=5.0.0,<6.0.0`	**6.0.0**	10/02/2025

5 exemple/psr7 2.4.0

1 avis · pire gravité : moyenne · licence MIT

P2

Exigé par : `exemple/http-client` (`^2.4`).

MOYENNE **Injection d'en-têtes ou de requêtes** CVE-2099-10003

Ce que cela permet : Des en-têtes ou des requêtes HTTP peuvent être falsifiés : empoisonnement du cache, détournement de réponses.

Intitulé de l'avis : Improper header validation allows CRLF injection

VERSIONS TOUCHÉES	CORRIGÉ EN	PUBLIÉ LE
`>=2.0.0,<2.4.5`	**2.4.5**	10/02/2025

6 exemple/debug-bar 1.2.0

1 avis · pire gravité : moyenne · développement · licence MIT

P3

Dépendance directe probable du projet (aucun autre paquet ne l'exige).

MOYENNE **Injection de script (XSS)** CVE-2099-10008

Ce que cela permet : Un attaquant peut faire exécuter du script dans le navigateur des visiteurs ou des administrateurs : vol de session, actions en leur nom, défiguration des pages.

Intitulé de l'avis : Cross-site scripting in the profiler panel

VERSIONS TOUCHÉES	CORRIGÉ EN	PUBLIÉ LE
<1.3.0	**1.3.0**	10/02/2025

7 exemple/yaml-parser 1.4.2

1 avis · pire gravité : faible · licence MIT

P3

Exigé par : drupal/core (~1.4.0).

FAIBLE **Fuite d'informations** CVE-2099-10007

Ce que cela permet : Des informations sensibles (identifiants, cookies, en-têtes d'autorisation, données internes) peuvent être exposées à un tiers.

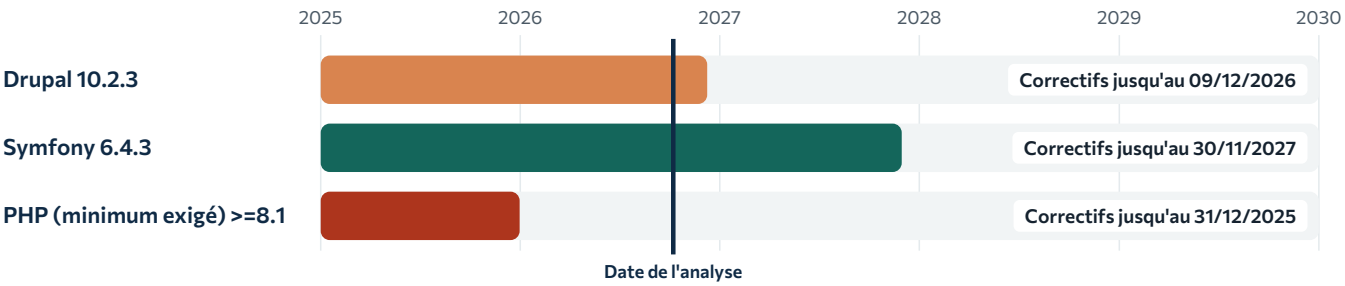
Intitulé de l'avis : Information disclosure in error messages

VERSIONS TOUCHÉES	CORRIGÉ EN	PUBLIÉ LE
>=1.0,<1.4.9|>=1.5,<1.5.2	**1.4.9**	10/02/2025

LOGICIELS DE BASE

Drupal, Symfony, PHP : jusqu'à quand sont-ils corrigés ?

Une version qui n'a plus de correctifs de sécurité accumule des failles qui ne seront jamais corrigées.



Drupal 10.2.3 FIN DE SUPPORT PROCHE

Fin des correctifs de sécurité le 09/12/2026 ; la montée de version est à planifier dès maintenant.

Symfony 6.4.3 SUPPORTÉE

Supportée : correctifs de sécurité jusqu'au 30/11/2027.

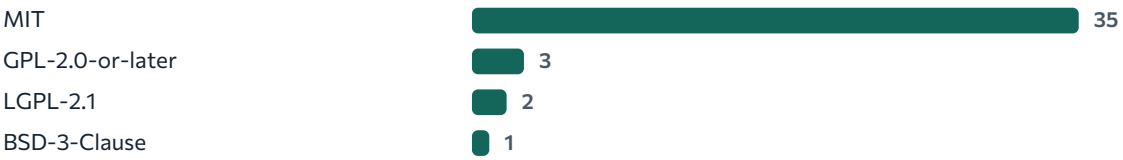
PHP (minimum exigé) >=8.1 PLUS SUPPORTÉE

Le projet accepte PHP 8.1 et plus. Pour cette branche, plus aucun correctif de sécurité depuis le 31/12/2025 ; les failles découvertes ne seront plus corrigées. La version réellement utilisée par le serveur est à vérifier.

PAQUETS ABANDONNÉS PAR LEURS AUTEURS

- `exemple/old-mailer` 3.1.0 : remplacement conseillé par l'auteur, `exemple/mailer`.

LICENCES DES PAQUETS DE PRODUCTION



Licences déclarées par les auteurs dans le composer.lock. Les licences copyleft (GPL, LGPL, AGPL) imposent des obligations en cas de redistribution : à vérifier selon votre usage.

MÉTHODE

Comment ce rapport a été établi

Ce qui a été fait, et ce qu'une analyse de dépendances ne peut pas dire.

EXEMPLE FICTIF

Ce projet et ses avis de sécurité (identifiants en 2099) n'existent pas : `drupal/core` et `symfony/http-kernel` sont de vrais paquets, mais leurs failles sont inventées. Données figées au 8 octobre 2026.

CE QUI A ÉTÉ FAIT

Les versions exactes installées ont été lues dans le composer.lock. Chaque paquet a été rapproché de la base publique d'avis de sécurité de Packagist (sources présentes dans ce rapport : Base fictive (exemple)). La version corrigée retenue est la première version publiée hors de toutes les plages touchées ; sa compatibilité avec les contraintes des paquets qui l'exigent a été vérifiée automatiquement.

LIRE LES GRAVITÉS

La gravité est celle publiée avec l'avis (échelle critique, élevée, moyenne, faible). Pour les avis de Drupal, à défaut, c'est le niveau de risque de l'équipe sécurité de Drupal. Le type de faille est déduit de l'intitulé de l'avis, pour aider la lecture. Les failles d'exécution de code et d'injection SQL en production sont toujours classées P1.

CE QUE CE RAPPORT NE DIT PAS

Une faille n'est réellement exploitable que si la fonction touchée est utilisée par le projet et accessible : cela demande un examen du code et de la configuration. Une faille sans avis publié n'est, par définition, pas détectée. La version de PHP réellement utilisée par le serveur n'est pas connue. Ce document ne remplace pas un test d'intrusion.

CONFIDENTIALITÉ

Le composer.lock n'a pas été conservé : seul ce rapport l'est, 180 jours au plus, sous un lien privé.

ANNEXE

Inventaire des paquets

Les 43 paquets du composer.lock, avec leur version exacte. Le même inventaire est livré au format CycloneDX (SBOM).

PAQUET	VERSION	USAGE	LICENCE	FAILLE
drupal/core	10.2.3	Prod.	GPL-2.0-or-later	Élevée
drupal/core-recommended	10.2.3	Prod.	GPL-2.0-or-later	
drupal/webform	6.2.2	Prod.	GPL-2.0-or-later	
exemple/font-lib	0.5.4	Prod.	LGPL-2.1	
exemple/http-client	7.5.1	Prod.	MIT	Critique
exemple/jwt	5.5.1	Prod.	BSD-3-Clause	Moyenne
exemple/lib-00	1.0.0	Prod.	MIT	
exemple/lib-01	1.1.0	Prod.	MIT	
exemple/lib-02	1.2.0	Prod.	MIT	
exemple/lib-03	1.3.0	Prod.	MIT	
exemple/lib-04	1.4.0	Prod.	MIT	
exemple/lib-05	1.5.0	Prod.	MIT	
exemple/lib-06	1.6.0	Prod.	MIT	
exemple/lib-07	1.7.0	Prod.	MIT	
exemple/lib-08	1.8.0	Prod.	MIT	
exemple/lib-09	1.9.0	Prod.	MIT	
exemple/lib-10	1.10.0	Prod.	MIT	
exemple/lib-11	1.11.0	Prod.	MIT	
exemple/lib-12	1.12.0	Prod.	MIT	
exemple/lib-13	1.13.0	Prod.	MIT	
exemple/lib-14	1.14.0	Prod.	MIT	
exemple/lib-15	1.15.0	Prod.	MIT	
exemple/lib-16	1.16.0	Prod.	MIT	
exemple/lib-17	1.17.0	Prod.	MIT	
exemple/lib-18	1.18.0	Prod.	MIT	
exemple/lib-19	1.19.0	Prod.	MIT	
exemple/lib-20	1.20.0	Prod.	MIT	
exemple/lib-21	1.21.0	Prod.	MIT	
exemple/lib-22	1.22.0	Prod.	MIT	
exemple/lib-23	1.23.0	Prod.	MIT	
exemple/lib-24	1.24.0	Prod.	MIT	
exemple/lib-25	1.25.0	Prod.	MIT	
exemple/lib-26	1.26.0	Prod.	MIT	
exemple/lib-27	1.27.0	Prod.	MIT	
exemple/lib-28	1.28.0	Prod.	MIT	
exemple/lib-29	1.29.0	Prod.	MIT	
exemple/old-mailer	3.1.0	Prod.	MIT	Abandonné
exemple/pdf-renderer	2.0.3	Prod.	LGPL-2.1	Critique
exemple/psr7	2.4.0	Prod.	MIT	Moyenne
exemple/yaml-parser	1.4.2	Prod.	MIT	Faible
symfony/http-kernel	v6.4.3	Prod.	MIT	
exemple/debug-bar	1.2.0	Dév.	MIT	Moyenne
exemple/test-runner	10.5.0	Dév.	MIT	