

PatchFirst — note de sécurité publique

2026-10-23 00:00 UTC · inventaire : acme-demo-2 · actifs : 4 · CVE.org sample-2026-10-23 · KEV 1754 · codes d'exploitation 1 CVE · sources non officielles en date du 2026-10-23 00:00

74_c

note du parc sur 100
production pondérée ×2

Note globale*: 74/100 (C)
23 composants vérifiés sur 23

1

P0 — urgent, 24 heures

9

P1 — une semaine

10

P2 — un mois

2

P3 — planifié

Notes les plus faibles : web-1.acme.example 37/100 E, app-1.acme.example 76/100 C, worker-1.acme.example 88/100 B, db-1.acme.example 96/100 A.

Redémarrez le service concerné après la mise à jour ; vérifiez la compatibilité et relancez une évaluation.

P0 — corriger aujourd’hui

SERVEUR	COMPOSANT	VERSION INSTALLÉE	MESURES À PRENDRE	EXPOSITION	ÉLÉMENTS PROBANTS
P0 web-1.acme.example	facade/ignition [composer] /var/www/shop/composer.lock	2.5.1	2.5.2	accessible publique-ment	CVE-2021-3129 · 9.8 KEV code d'exploitation : metasploit

Notes par actif

ACTIF	NOTE		P0	P1	P2	P3	SYSTÈME	SERVICES PUBLICS
web-1.acme.example	37 Note globale*: 37/100 (E) 7 composants vérifiés sur 7	E	1	5	1	·	Ubuntu 22.04 LTS	web (nginx)
app-1.acme.example	76 Note globale*: 76/100 (C) 8 composants vérifiés sur 8	C	·	3	4	·	Debian GNU/Linux 12	web (node)
worker-1.acme.example	88 Note globale*: 88/100 (B) 6 composants vérifiés sur 6	B	·	1	3	2	Debian GNU/Linux 12	

ACTIF	NOTE		P0	P1	P2	P3	SYSTÈME	SERVICES PUBLICS
db-1.acme.example	96 A		.	.	2	.	Debian GNU/Linux 12	
	Note globale*: 96/100 (A) 2 composants vérifiés sur 2							

Méthodologie

Risque = gravité × exploitabilité × exposition. La gravité utilise la priorité Ubuntu/Debian ou, à défaut, CVSS. Exploitabilité : CISA KEV ×2, exploitation CIRCL ou SSVc ×1,7, code d'exploitation public/PoC ×1,4, EPSS ≥10 % ×1,3, discussion ×1,1. Exposition : publique 1,0 · potentiellement publique 0,8 · interne 0,6 · locale 0,45.

Priorité : P0 — risque ≥14 ou KEV sur un service public (24 heures) · P1 — ≥8 ou toute KEV (une semaine) · P2 — ≥4 (un mois) · P3 — planifié.

Note de l'actif : 100 moins les pénalités des constats ; plafonnée à 49 dès qu'un P0 est présent. A ≥90 · B ≥80 · C ≥65 · D ≥50 · E ≥35 · F.

Sources utilisées : CVE.org, OSV.dev (paquets Ubuntu/Debian avec correctifs rétroportés, Composer), CISA KEV, FIRST EPSS, Exploit-DB, Metasploit, Nuclei, CIRCL Vulnerability-Lookup, endoflife.date. Les paquets de dépôts tiers (comme sury PPA) sont vérifiés à l'aide des versions du projet d'origine.

P1 — sous une semaine

web-1.acme.example · 5

	COMPOSANT	VERSION INSTALLÉE	MESURES À PRENDRE	EXPOSITION	ÉLÉMENTS PROBANTS
P1	php8.1 php8.1-fpm	8.1.2-1ubuntu2	8.1.2-1ubuntu2.28	accessible publique- ment	CVE-2026-109618 · 9.5 +65 CVE
P1	league/commonmark [composer] /var/www/shop/composer.lock	2.6.0	2.10.2	accessible publique- ment	CVE-2026-105830 · 8.7 +13 CVE
P1	twig/twig [composer] /var/www/shop/composer.lock	3.14.0	3.27.0	accessible publique- ment	CVE-2026-24425 · 8.7 +14 CVE
P1	guzzlehttp/guzzle [composer] /var/www/shop/composer.lock	7.4.1	7.15.2	accessible publique- ment	CVE-2026-67354 · 8.2 +13 CVE
P1	nginx nginx	1.18.0- 6ubuntu14	1.18.0-6ubuntu14.21	accessible publique- ment	CVE-2026-42945 · 8.0 +33 CVE

app-1.acme.example · 3

	COMPOSANT	VERSION INSTALLÉE	MESURES À PRENDRE	EXPOSITION	ÉLÉMENTS PROBANTS
P1	lodash [npm] /srv/catalog/package-lock.json	4.17.20	4.18.0	accessible publique- ment	CVE-2021-23337 · 7.2 +4 CVE code d'exploitation : PoC
P1	nodejs nodejs	18.19.0+dfsg-6~deb12u2	18.20.4+dfsg-1~deb12u3	accessible publique- ment	CVE-2026-111497 · 9.2 +41 CVE
P1	axios [npm] /srv/catalog/package-lock.json	1.7.8	1.20.0	accessible publique- ment	CVE-2026-44494 · 8.7 +32 CVE

worker-1.acme.example · 1

	COMPOSANT	VERSION INSTALLÉE	MESURES À PRENDRE	EXPOSITION	ÉLÉMENTS PROBANTS
P1	nginx nginx	1.22.1-9+deb12u2	1.22.1-9+deb12u10	interne	CVE-2023-44487 · 7.5 +24 CVE KEV

P2 — mises à jour planifiées ce mois-ci

web-1.acme.example · 1

	COMPOSANT	VERSION INSTALLÉE	MESURES À PRENDRE	EXPOSITION	ÉLÉMENTS PROBANTS
P2	symfony/http-foundation [composer] /var/www/shop/composer.lock	5.4.45	5.4.50	accessible publique- ment	CVE-2025-64500 · 7.3 +1 CVE

app-1.acme.example · 4

	COMPOSANT	VERSION INSTALLÉE	MESURES À PRENDRE	EXPOSITION	ÉLÉMENTS PROBANTS
P2	path-to-regexp [npm] /srv/catalog/package-lock.json	0.1.11	0.1.13	accessible publique- ment	CVE-2024-52798 · 7.7 +2 CVE
P2	ws [npm] /srv/catalog/package-lock.json	8.17.0	8.21.0	accessible publique- ment	CVE-2024-37890 · 7.5 +2 CVE
P2	jsonwebtoken [npm] /srv/catalog/package-lock.json	8.5.1	9.0.0	accessible publique- ment	CVE-2022-23540 · 6.4 +2 CVE
P2	semver [npm] /srv/catalog/package-lock.json	7.5.1	7.5.2	accessible publique- ment	CVE-2022-25883 · 5.3

worker-1.acme.example · 3

	COMPOSANT	VERSION INSTALLÉE	MESURES À PRENDRE	EXPOSITION	ÉLÉMENTS PROBANTS
P2	django [PyPI] /srv/jobs/requirements.txt	4.2.20	5.2.17	interne	CVE-2026-4277 · 9.8 +29 CVE
P2	pillow [PyPI] /srv/jobs/requirements.txt	10.3.0	13.0.0	interne	CVE-2026-112393 · 9.2 +50 CVE
P2	urllib3 [PyPI] /srv/jobs/requirements.txt	2.2.1	2.8.0	interne	CVE-2025-66471 · 8.9 +8 CVE

db-1.acme.example · 2

	COMPOSANT	VERSION INSTALLÉE	MESURES À PRENDRE	EXPOSITION	ÉLÉMENTS PROBANTS
P2	postgresql-15 postgresql-15	15.3-0+deb12u1	15.19-0+deb12u1	interne	CVE-2023-5869 · 8.8 +55 CVE
P2	redis redis-server	5:7.0.15- 1~deb12u1	5:7.0.15-1~deb12u10	accès local	CVE-2025-49844 · 10.0 +25 CVE

P3 — maintenance courante

worker-1.acme.example · 2

	COMPOSANT	VERSION INSTALLÉE	MESURES À PRENDRE	EXPOSITION	ÉLÉMENTS PROBANTS
P3	jinja2 [PyPI] /srv/jobs/requirements.txt	3.1.4	3.1.6	interne	CVE-2025-27516 · 5.4 +2 CVE
P3	requests [PyPI] /srv/jobs/requirements.txt	2.32.2	2.33.0	interne	CVE-2024-47081 · 5.3 +1 CVE

* La note globale considère les composants non vérifiés comme un risque inconnu. [Calcul de la note globale.](#)