

PatchFirst — Bewertung der öffentlichen Angriffsfläche

2026-10-23 00:00 UTC · Inventarstand: acme-demo-2 · Systeme: 4 · CVE.org sample-2026-10-23 · KEV 1754 · verfügbare Exploits 1 CVE · inoffizielle Quellen, Stand 2026-10-23 00:00

74_c

Bewertung des Serverbestands von 100
Produktion doppelt gewichtet ×2

Gesamtbewertung*: 74/100 (C)
23 von 23 Komponenten geprüft

1

P0 —
dringend, 24
Stunden

9

P1 — eine
Woche

10

P2 — ein
Monat

2

P3 — geplant

Niedrigste Bewertungen: 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.

Starten Sie den betroffenen Dienst nach dem Update neu, prüfen Sie die Kompatibilität und führen Sie eine erneute Bewertung durch.

P0 — heute patchen

SERVERINSTANZ	KOMPONENTE	VERSIONS-STAND	MASSNAHME	ERREICH-BARKEIT	NACHWEISE
P0 web-1.acme.example	facade/ignition [composer] /var/www/shop/composer.lock	2.5.1	2.5.2	öffentlich	CVE-2021-3129 · 9.8 KEV Exploit verfügbar: metasploit

Bewertungen nach System

IT-SYSTEM	BEWERTUNG	P0	P1	P2	P3	BETRIEBSSYSTEM	ÖFFENTLICH ERREICHBARE DIENSTE
web-1.acme.example	37 E Gesamtbewertung*: 37/100 (E) 7 von 7 Komponenten geprüft	1	5	1	·	Ubuntu 22.04 LTS	web (nginx)
app-1.acme.example	76 C Gesamtbewertung*: 76/100 (C) 8 von 8 Komponenten geprüft	·	3	4	·	Debian GNU/Linux 12	web (node)

IT-SYSTEM	BEWERTUNG	P0	P1	P2	P3	BETRIEBSSYSTEM	ÖFFENTLICH ERREICHBARE DIENSTE
worker-1.acme.example	88 B Gesamt- bewertung*: 88/100 (B) 6 von 6 Komponenten geprüft	.	1	3	2	Debian GNU/Linux 12	
db-1.acme.example	96 A Gesamt- bewertung*: 96/100 (A) 2 von 2 Komponenten geprüft	.	.	2	.	Debian GNU/Linux 12	

Methodik

Risiko = Schweregrad × Ausnutzbarkeit × Erreichbarkeit. Schweregrad nach Ubuntu-/Debian-Priorität, sonst CVSS. Ausnutzbarkeit: CISA KEV ×2, CIRCL- oder SSVC-Ausnutzung ×1,7, öffentlicher Exploit/PoC ×1,4, EPSS ≥10 % ×1,3, Diskussion ×1,1. Erreichbarkeit: öffentlich 1,0 · möglicherweise öffentlich 0,8 · intern 0,6 · lokal 0,45.

Priorität: P0 — Risiko ≥14 oder KEV bei öffentlich erreichbarem Dienst (24 Stunden) · P1 — ≥8 oder beliebiger KEV-Eintrag (eine Woche) · P2 — ≥4 (ein Monat) · P3 — geplant.

Systembewertung: 100 abzüglich Befundabzügen; bei P0 auf höchstens 49 begrenzt. A ≥90 · B ≥80 · C ≥65 · D ≥50 · E ≥35 · F.

Quellen: CVE.org, OSV.dev (Ubuntu-/Debian-Pakete mit Backports, Composer), CISA KEV, FIRST EPSS, Exploit-DB, Metasploit, Nuclei, CIRCL Vulnerability-Lookup, endoflife.date. Pakete aus Drittanbieter-Repositories (etwa sury PPA) werden anhand ihrer Upstream-Versionen geprüft.

P1 — innerhalb einer Woche

web-1.acme.example · 5

	KOMPONENTE	VERSIONSSTAND	MASSNAHME	ERREICH- BARKEIT	NACHWEISE
P1	php8.1 php8.1-fpm	8.1.2-1ubuntu2	8.1.2-1ubuntu2.28	öffentlich	CVE-2026-109618 · 9.5 +65 CVE
P1	league/commonmark [composer] /var/www/shop/composer.lo ck	2.6.0	2.10.2	öffentlich	CVE-2026-105830 · 8.7 +13 CVE
P1	twig/twig [composer] /var/www/shop/composer.lo ck	3.14.0	3.27.0	öffentlich	CVE-2026-24425 · 8.7 +14 CVE
P1	guzzlehttp/guzzle [composer] /var/www/shop/composer.lo ck	7.4.1	7.15.2	öffentlich	CVE-2026-67354 · 8.2 +13 CVE
P1	nginx nginx	1.18.0- 6ubuntu14	1.18.0-6ubuntu14.21	öffentlich	CVE-2026-42945 · 8.0 +33 CVE

app-1.acme.example · 3

	KOMPONENTE	VERSIONSSTAND	MASSNAHME	ERREICH-BARKEIT	NACHWEISE
P1	lodash [npm] /srv/catalog/package-lock.json	4.17.20	4.18.0	öffentlich	CVE-2021-23337 · 7.2 +4 CVE Exploit verfügbar: PoC
P1	nodejs nodejs	18.19.0+dfsg-6~deb12u2	18.20.4+dfsg-1~deb12u3	öffentlich	CVE-2026-111497 · 9.2 +41 CVE
P1	axios [npm] /srv/catalog/package-lock.json	1.7.8	1.20.0	öffentlich	CVE-2026-44494 · 8.7 +32 CVE

worker-1.acme.example · 1

	KOMPONENTE	VERSIONSSTAND	MASSNAHME	ERREICH-BARKEIT	NACHWEISE
P1	nginx nginx	1.22.1-9+deb12u2	1.22.1-9+deb12u10	intern	CVE-2023-44487 · 7.5 +24 CVE KEV

P2 — geplante Updates in diesem Monat

web-1.acme.example · 1

	KOMPONENTE	VERSIONSSTAND	MASSNAHME	ERREICH-BARKEIT	NACHWEISE
P2	symfony/http-foundation [composer] /var/www/shop/composer.lock	5.4.45	5.4.50	öffentlich	CVE-2025-64500 · 7.3 +1 CVE

app-1.acme.example · 4

	KOMPONENTE	VERSIONSSTAND	MASSNAHME	ERREICH-BARKEIT	NACHWEISE
P2	path-to-regexp [npm] /srv/catalog/package-lock.json	0.1.11	0.1.13	öffentlich	CVE-2024-52798 · 7.7 +2 CVE
P2	ws [npm] /srv/catalog/package-lock.json	8.17.0	8.21.0	öffentlich	CVE-2024-37890 · 7.5 +2 CVE
P2	jsonwebtoken [npm] /srv/catalog/package-lock.json	8.5.1	9.0.0	öffentlich	CVE-2022-23540 · 6.4 +2 CVE
P2	semver [npm] /srv/catalog/package-lock.json	7.5.1	7.5.2	öffentlich	CVE-2022-25883 · 5.3

worker-1.acme.example · 3

	KOMPONENTE	VERSIONSSTAND	MASSNAHME	ERREICH-BARKEIT	NACHWEISE
P2	django [PyPI] /srv/jobs/requirements.txt	4.2.20	5.2.17	intern	CVE-2026-4277 · 9.8 +29 CVE
P2	pillow [PyPI] /srv/jobs/requirements.txt	10.3.0	13.0.0	intern	CVE-2026-112393 · 9.2 +50 CVE
P2	urllib3 [PyPI] /srv/jobs/requirements.txt	2.2.1	2.8.0	intern	CVE-2025-66471 · 8.9 +8 CVE

db-1.acme.example · 2

	KOMPONENTE	VERSIONSSTAND	MASSNAHME	ERREICH-BARKEIT	NACHWEISE
P2	postgresql-15 postgresql-15	15.3-0+deb12u1	15.19-0+deb12u1	intern	CVE-2023-5869 · 8.8 +55 CVE
P2	redis redis-server	5:7.0.15- 1~deb12u1	5:7.0.15-1~deb12u10	lokal	CVE-2025-49844 · 10.0 +25 CVE

P3 — reguläre Wartung

worker-1.acme.example · 2

	KOMPONENTE	VERSIONSSTAND	MASSNAHME	ERREICH-BARKEIT	NACHWEISE
P3	jinja2 [PyPI] /srv/jobs/requirements.txt	3.1.4	3.1.6	intern	CVE-2025-27516 · 5.4 +2 CVE
P3	requests [PyPI] /srv/jobs/requirements.txt	2.32.2	2.33.0	intern	CVE-2024-47081 · 5.3 +1 CVE

* Die Gesamtbewertung berücksichtigt ungeprüfte Komponenten als unbekanntes Risiko. So wird die Gesamtbewertung berechnet.