

Scan rapide de Exemple SARL

Serveur : surveillance@serveur-web:22

Scan terminé le 26/10/2026 07:04

Rapport généré le 26/10/2026 07:10

Résumé

14 failles connues dans les composants installés, chaque emplacement compté :

3 de gravité critique

5 de gravité haute

4 de gravité moyenne

2 de gravité faible

6 mises à jour corrigent des failles critiques ou hautes : elles sont détaillées plus bas, les plus urgentes d'abord.

Depuis le scan du 19/10/2026 08:03 : 4 failles corrigées (dont 0 critique, 2 hautes), 4 failles apparues (dont 2 critiques, 1 haute).

Par emplacement

Emplacement	Critiques	Hautes	Total
fichier /srv/boutique/package-lock.json	1	2	5
hôte du serveur	1	1	5
conteneur site-web	1	1	2
conteneur back-office	0	1	2

Mises à jour prioritaires, les plus urgentes d'abord

CRITIQUE : jsonwebtoken 8.5.1 (npm)

Où : fichier /srv/boutique/package-lock.json

Faillles corrigées : 1 critique, 1 haute, 0 autre

Mettre à jour vers la version 9.0.3 ou plus récente.

Ce que c'est

Cette bibliothèque vérifie les jetons de connexion de votre boutique en ligne : c'est elle qui décide si un visiteur est bien connecté à son compte client ou au compte administrateur.

Ce que vous risquez

Un pirate pourrait fabriquer un faux jeton et se faire passer pour n'importe quel utilisateur, y compris un administrateur de la boutique : accès aux commandes, aux adresses et aux coordonnées des clients.

Faillles les plus graves : GHSA-8c4v-2q7w-m9fx et GHSA-3hr7-x5p2-c6wq

GHSA-8c4v-2q7w-m9fx : Signature verification can be bypassed with a crafted token header

CRITIQUE : openssl 3.0.13-0ubuntu3.4 (Ubuntu:24.04:LTS)

Où : hôte du serveur

Faillles corrigées : 1 critique, 0 haute, 1 autre

Mettre à jour vers la version 3.0.13-0ubuntu3.6 ou plus récente.

Ce que c'est

OpenSSL chiffre les échanges entre votre serveur et ses visiteurs : c'est lui qui affiche le cadenas dans le navigateur. Cette copie est celle du serveur lui-même.

Ce que vous risquez

Un pirate pourrait, en envoyant un certificat piégé, prendre le contrôle du programme qui l'analyse, donc d'une partie du serveur, sans avoir besoin de mot de passe. Ce type de faille est exploité par des robots dans les jours qui suivent sa publication.

Faillles les plus graves : UBUNTU-CVE-2026-31842

UBUNTU-CVE-2026-31842 : Buffer overflow when processing crafted certificates may allow remote code execution

CRITIQUE : openssl 3.0.15-1~deb12u1 (Debian:12)

Où : conteneur site-web

Faillles corrigées : 1 critique, 0 haute, 0 autre

Mettre à jour vers la version 3.0.17-1~deb12u2 ou plus récente.

Ce que c'est

La même faille d'OpenSSL, dans une autre copie : celle qu'embarque le conteneur du site web. Mettre à jour le serveur ne suffit pas, l'image du conteneur doit être reconstruite.

Ce que vous risquez

Le même que pour le serveur, limité au site web : un pirate pourrait en prendre le contrôle.

Faillles les plus graves : DEBIAN-CVE-2026-31842

HAUTE : libxml2 2.9.14+dfsg-1.3~deb12u1 (Debian:12)

Où : conteneur back-office et conteneur site-web

Faillles corrigées : 0 critique, 1 haute, 0 autre

Mettre à jour vers la version 2.9.14+dfsg-1.3~deb12u3 ou plus récente.

Ce que c'est

libxml2 lit les fichiers au format XML, par exemple les flux de produits ou les exports échangés avec vos partenaires. Elle est présente dans les conteneurs du site web et du back-office.

Ce que vous risquez

Un fichier XML piégé pourrait faire planter l'application, voire permettre à un pirate d'y exécuter ses propres commandes.

Faillles les plus graves : DEBIAN-CVE-2026-24410

HAUTE : multer 1.4.5-lts.1 (npm)

Où : fichier /srv/boutique/package-lock.json

Faillles corrigées : 0 critique, 1 haute, 0 autre

Mettre à jour vers la version 2.0.4 ou plus récente.

Ce que c'est

Multer reçoit les fichiers envoyés par les visiteurs de la boutique, comme une pièce jointe au formulaire de contact.

Ce que vous risquez

Une seule requête mal formée suffit à faire tomber la boutique : elle reste indisponible jusqu'à son redémarrage. Votre site peut être mis hors ligne à volonté.

Faillles les plus graves : GHSA-q4jm-7v9c-wr2h

GHSA-q4jm-7v9c-wr2h : Malformed multipart request causes an unhandled exception and crashes the process

HAUTE : openssh-server 1:9.6p1-3ubuntu13.5 (Ubuntu:24.04:LTS)

Où : hôte du serveur

Faillles corrigées : 0 critique, 1 haute, 0 autre

Mettre à jour vers la version 1:9.6p1-3ubuntu13.9 ou plus récente.

Ce que c'est

OpenSSH est la porte d'entrée par laquelle votre prestataire administre le serveur à distance.

Ce que vous risquez

Dans certaines conditions, un pirate pourrait ouvrir cette porte sans connaître de mot de passe. L'attaque est difficile à réussir, mais elle se tente automatiquement et sans relâche.

Faillles les plus graves : UBUNTU-CVE-2026-27455

UBUNTU-CVE-2026-27455 : Race condition in signal handler may allow unauthenticated remote code execution

Autres mises à jour

5 autres composants n'ont que des failles moyennes ou faibles (5 au total) : à traiter lors des mises à jour habituelles du serveur et des images.

Conteneurs à surveiller

Image construite sur le serveur à laquelle manquent des correctifs publiés depuis plus de 30 jours : à reconstruire sans cache.

back-office