KINLEY MARKETING SECURITY
CYBERSÉCURITÉ · AUDIT · CONSEIL

EXEMPLE

SYNTHÈSE EXÉCUTIVE

RAPPORT D'AUDIT DE SÉCURITÉ

Analyse réalisée avec KINLEYAUDIT

Entreprise exemple

DATE DE L'AUDIT	26/11/2026 à 12:12 (heure de Paris)
PÉRIMÈTRE AUDITÉ	1 serveur
RAPPORT ÉTABLI LE	27/11/2026 à 13:49 (heure de Paris)



ÉTAT DE SÉCURITÉ

B · 88,7

Risque modéré



HYGIÈNE DE MAINTENANCE

A · 100,0

0 action à mener

Exemple de rapport : données anonymisées, issues d'un audit réel. Aucune information du client d'origine n'y figure.

1 Synthèse exécutive



NOTE 1 · ÉTAT DE SÉCURITÉ

RISQUE MODÉRÉ

Le risque présent sur le serveur, avec ou sans correctif disponible.



NOTE 2 · HYGIÈNE DE MAINTENANCE

0 ACTION À MENER

Ce qui est à votre main : mises à jour et redémarrage non appliqués.

En clair

Le périmètre audité présente 695 vulnérabilités confirmées touchant 35 logiciels, dont 20 critiques et 228 élevées. Toutefois, aucune ne dispose actuellement d'un correctif installable depuis les dépôts standard : 695 nécessitent la publication d'un correctif par Ubuntu ou l'éditeur concerné.

Ce niveau décrit le risque présent sur le serveur ; il ne signale pas de mises à jour oubliées : aucun correctif standard n'est disponible à ce jour.

370 résultats restent en attente de qualification par Ubuntu : ils ne sont pas des vulnérabilités avérées ni comptés dans la note, mais leur confirmation éventuelle pourrait dégrader celle-ci.

Vulnérabilités confirmées par criticité — 695 au total (gravité technique CVSS ; définitions en section 7)

20	228	266	180	1
Critiques	Élevées	Moyennes	Faibles	Non classées

Que peut-on corriger aujourd'hui ? — capacité de remédiation à la date de l'audit

0	0	695
Correctif immédiat	**Via Ubuntu Pro**	**Correctif externe**
installable depuis les dépôts standard	remédiation possible, activation à décider	attendu d'Ubuntu ou de l'éditeur

À part : 370 résultats en attente de qualification par Ubuntu (non confirmés, hors de ces décomptes et hors note).

Principaux risques constatés

- 20 vulnérabilités critiques confirmées, principalement dans : linux, libslang2.
- 228 vulnérabilités élevées confirmées.
- L'accès SSH par mot de passe est autorisé (recommandation de durcissement).

Actions prioritaires

- Durcir l'accès SSH selon l'usage réel (clés uniquement, limitation du port, surveillance des tentatives).

Sommaire

1 Synthèse exécutive 2
2 Priorités de sécurité 4
3 État global de sécurité 7
4 Capacité de remédiation 9
5 Logiciels les plus concernés 10
6 Recommandations 12
7 Méthodologie, limites et glossaire 13

ANNEXES

Annexe A — Sources et références 16

Les annexes conservent les données de référence à l'usage de l'administrateur système ou du RSSI ; les sections numérotées en présentent l'interprétation. Les détails d'infrastructure (adresses, services, ports, configurations) figurent uniquement dans le rapport technique.

2 Priorités de sécurité

Les points qui méritent une attention particulière, classés par gravité puis par possibilité d'action. Seuls figurent ici des risques **confirmés** ou des constats de configuration : un résultat non confirmé n'est jamais présenté comme un incident. Le score CVSS (de 0 à 10) mesure la gravité technique théorique d'une faille ; il ne prouve pas qu'elle soit exploitable sur ce serveur.

Serveur 1 — Serveur 1 (OS masqué)

CVE-2026-72200 — linux 7.0.0-44.44 Critique CVSS 9,8

Machine concernée : **Serveur 1 — Serveur 1**

GRAVITÉ THÉORIQUE	Selon le vecteur CVSS (théorique) : attaque possible par le réseau, sans authentification ; impact élevé sur la confidentialité, l'intégrité et la disponibilité.
APPLICABILITÉ	Confirmée par Ubuntu pour la version installée
ACCESSIBILITÉ DU COMPOSANT	Non établie par l'audit
EXPLOITATION RÉELLE	Non vérifiée dans l'environnement audité
ACTION	Surveiller la publication d'un correctif Ubuntu ; limiter l'exposition du service en attendant.
QUI PEUT AGIR	**Ubuntu**

CVE-2026-99304 — linux 7.0.0-44.44 Critique CVSS 9,8

Machine concernée : **Serveur 1 — Serveur 1**

GRAVITÉ THÉORIQUE	Selon le vecteur CVSS (théorique) : attaque possible par le réseau, sans authentification ; impact élevé sur la confidentialité, l'intégrité et la disponibilité.
APPLICABILITÉ	Confirmée par Ubuntu pour la version installée
ACCESSIBILITÉ DU COMPOSANT	Non établie par l'audit
EXPLOITATION RÉELLE	Non vérifiée dans l'environnement audité
ACTION	Surveiller la publication d'un correctif Ubuntu ; limiter l'exposition du service en attendant.
QUI PEUT AGIR	**Ubuntu**

CVE-2026-99306 — linux 7.0.0-44.44 Critique CVSS 9,8

Machine concernée : **Serveur 1 — Serveur 1**

GRAVITÉ THÉORIQUE	Selon le vecteur CVSS (théorique) : attaque possible par le réseau, sans authentification ; impact élevé sur la confidentialité, l'intégrité et la disponibilité.
APPLICABILITÉ	Confirmée par Ubuntu pour la version installée
ACCESSIBILITÉ DU COMPOSANT	Non établie par l'audit
EXPLOITATION RÉELLE	Non vérifiée dans l'environnement audité
ACTION	Surveiller la publication d'un correctif Ubuntu ; limiter l'exposition du service en attendant.
QUI PEUT AGIR	**Ubuntu**

CVE-2026-99310 — linux 7.0.0-44.44 Critique CVSS 9,8

Machine concernée : **Serveur 1 — Serveur 1**

GRAVITÉ THÉORIQUE	Selon le vecteur CVSS (théorique) : attaque possible par le réseau, sans authentification ; impact élevé sur la confidentialité, l'intégrité et la disponibilité.
APPLICABILITÉ	Confirmée par Ubuntu pour la version installée
ACCESSIBILITÉ DU COMPOSANT	Non établie par l'audit
EXPLOITATION RÉELLE	Non vérifiée dans l'environnement audité
ACTION	Surveiller la publication d'un correctif Ubuntu ; limiter l'exposition du service en attendant.
QUI PEUT AGIR	**Ubuntu**

CVE-2026-99356 — linux 7.0.0-44.44 Critique CVSS 9,8

Machine concernée : **Serveur 1 — Serveur 1**

GRAVITÉ THÉORIQUE	Selon le vecteur CVSS (théorique) : attaque possible par le réseau, sans authentification ; impact élevé sur la confidentialité, l'intégrité et la disponibilité.
APPLICABILITÉ	Confirmée par Ubuntu pour la version installée
ACCESSIBILITÉ DU COMPOSANT	Non établie par l'audit
EXPLOITATION RÉELLE	Non vérifiée dans l'environnement audité
ACTION	Surveiller la publication d'un correctif Ubuntu ; limiter l'exposition du service en attendant.
QUI PEUT AGIR	**Ubuntu**

CVE-2026-99362 — linux 7.0.0-44.44 Critique CVSS 9,8

Machine concernée : **Serveur 1 — Serveur 1**

GRAVITÉ THÉORIQUE	Selon le vecteur CVSS (théorique) : attaque possible par le réseau, sans authentification ; impact élevé sur la confidentialité, l'intégrité et la disponibilité.
APPLICABILITÉ	Confirmée par Ubuntu pour la version installée
ACCESSIBILITÉ DU COMPOSANT	Non établie par l'audit
EXPLOITATION RÉELLE	Non vérifiée dans l'environnement audité
ACTION	Surveiller la publication d'un correctif Ubuntu ; limiter l'exposition du service en attendant.
QUI PEUT AGIR	**Ubuntu**

CVE-2026-99366 — linux 7.0.0-44.44 Critique CVSS 9,8

Machine concernée : **Serveur 1 — Serveur 1**

GRAVITÉ THÉORIQUE	Selon le vecteur CVSS (théorique) : attaque possible par le réseau, sans authentification ; impact élevé sur la confidentialité, l'intégrité et la disponibilité.
APPLICABILITÉ	Confirmée par Ubuntu pour la version installée
ACCESSIBILITÉ DU COMPOSANT	Non établie par l'audit
EXPLOITATION RÉELLE	Non vérifiée dans l'environnement audité
ACTION	Surveiller la publication d'un correctif Ubuntu ; limiter l'exposition du service en attendant.
QUI PEUT AGIR	**Ubuntu**

CVE-2026-99385 — linux 7.0.0-44.44 Critique CVSS 9,8

Machine concernée : **Serveur 1 — Serveur 1**

GRAVITÉ THÉORIQUE	Selon le vecteur CVSS (théorique) : attaque possible par le réseau, sans authentification ; impact élevé sur la confidentialité, l'intégrité et la disponibilité.
APPLICABILITÉ	Confirmée par Ubuntu pour la version installée
ACCESSIBILITÉ DU COMPOSANT	Non établie par l'audit
EXPLOITATION RÉELLE	Non vérifiée dans l'environnement audité
ACTION	Surveiller la publication d'un correctif Ubuntu ; limiter l'exposition du service en attendant.
QUI PEUT AGIR	**Ubuntu**

13 autre points de même nature sur ce serveur sont détaillés dans l'analyse des vulnérabilités et les annexes.

Failles élevées confirmées sur le serveur 1, par logiciel

LOGICIEL	FAILLES	ACTION	QUI PEUT AGIR
linux	188	Attendre le correctif d'Ubuntu ; limiter l'exposition.	Ubuntu
linux	17	Attendre le correctif de l'éditeur ; évaluer l'isolement.	Éditeur / mainteneur amont
binutils	3	Attendre le correctif d'Ubuntu ; limiter l'exposition.	Ubuntu
isc-dhcp-common	3	Attendre le correctif d'Ubuntu ; limiter l'exposition.	Ubuntu
libsqlite3-0	3	Attendre le correctif d'Ubuntu ; limiter l'exposition.	Ubuntu
perl	3	Attendre le correctif de l'éditeur ; évaluer l'isolement.	Éditeur / mainteneur amont

9 autres logiciels concernés sur ce serveur : voir l'analyse des vulnérabilités.

3 État global de sécurité

Deux notes complémentaires. L'**état de sécurité** mesure le risque présent sur le périmètre, à partir des seules vulnérabilités confirmées. L'**hygiène de maintenance** mesure ce que l'administrateur peut corriger aujourd'hui et n'a pas fait ; le détail figure en section 4. Un risque peut exister sans qu'aucun correctif ne soit disponible : ce n'est alors pas un oubli de l'administrateur.

Note 1 — État de sécurité : B (88,7 / 100)

Mesure le **risque présent**. Chaque **logiciel** vulnérable compte **une seule fois**, selon sa faille confirmée la plus grave : plusieurs milliers de CVE d'un même noyau se corrigent par la même mise à jour et ne doivent pas à elles seules faire s'effondrer la note. Ici, 35 logiciels vulnérables.

CATÉGORIE	NOMBRE	POINTS PAR UNITÉ	POINTS CALCULÉS	PLAFOND	POINTS PERDUS
Logiciels dont la pire faille est critique	2	2,0	4,0	30	**4,0**
Logiciels dont la pire faille est élevée	13	0,5	6,5	20	**6,5**
Logiciels dont la pire faille est moyenne	17	0,1	0,9	5	**0,9**
100 − total des points perdus (11,3) =					**88,7**

Lettre : `A ≥ 90 · B ≥ 75 · C ≥ 60 · D ≥ 40 · F < 40`. Niveau de risque associé : **modéré**. La note compte **toutes** les failles confirmées, **avec ou sans correctif**, mais jamais les 370 résultats en attente de qualification, les 0 paquet obsolète ni les résultats écartés par Ubuntu. Si une partie des résultats en attente était confirmée, la note pourrait baisser.

Note 2 — Hygiène de maintenance : A (100,0 / 100)

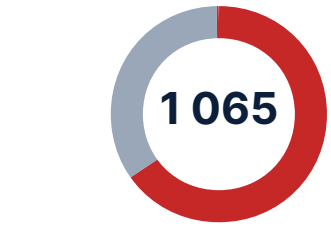
Mesure ce qui est **à la main de l'administrateur** : les mises à jour des dépôts standard et le redémarrage disponibles mais non appliqués. Chaque **action** (un logiciel à mettre à jour, ou un redémarrage) compte une fois, selon la faille la plus grave qu'elle corrige. Un correctif via Ubuntu Pro, ou pas encore publié par Ubuntu, n'est **pas** une négligence et n'est pas compté.

CATÉGORIE	ACTIONS	POINTS PAR ACTION	POINTS CALCULÉS	PLAFOND	POINTS PERDUS
Actions corrigeant une faille critique	0	10,0	0,0	60	**0,0**
Actions corrigeant une faille élevée	0	3,0	0,0	30	**0,0**
Actions corrigeant une faille moyenne	0	0,5	0,0	10	**0,0**
100 − total des points perdus (0,0) =					**100,0**

Aucune mise à jour ni redémarrage disponible n'est en attente d'application.

> **Pourquoi deux notes ?**
> Un serveur peut être à jour (bonne hygiène) tout en présentant un risque élevé parce que des failles n'ont pas encore de correctif ; à l'inverse, une mauvaise hygiène se corrige par des actions précises. Les deux notes se lisent toujours ensemble.

Comprendre les totaux

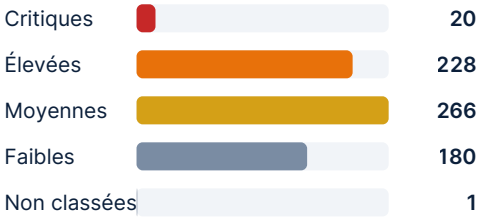


- 695 confirmées
- 370 en attente de qualification
- 0 paquet obsolète

Résultats recensés par l'audit	**1 065**
dont vulnérabilités confirmées et applicables	695
dont résultats en attente de qualification (non confirmés)	370
dont paquets obsolètes hors dépôts (non évaluables)	0
Résultats actifs (confirmés + en attente, hors paquets obsolètes)	**1 065**
Résultats écartés par Ubuntu, jamais comptés	8
dont déjà corrigés (y compris correctifs rétroportés) : 0 · non concernés : 0 · ignorés : 8	

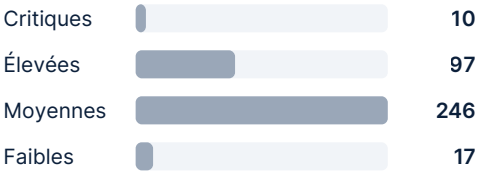
Le total des « résultats actifs » est celui retenu pour l'historique des audits ; les graphiques par criticité ci-dessous séparent toujours les résultats confirmés des résultats non qualifiés.

Confirmées, par criticité — 695



Applicables à la version installée, confirmées par Ubuntu.

En attente de qualification — 370



Non confirmées : criticité théorique (score CVSS générique), hors note.

Situation par serveur

SERVEUR	ÉTAT DE SÉCURITÉ	MAINTENANCE	CONFIRMÉES	DONT CRIT. / ÉLEVÉES	CORRECTIF STANDARD	VIA PRO	CORRECTIF EXTERNE	EN ATTENTE
Serveur 1 Ubuntu 26.04.1 LTS	B 88,7	A 0 action	695	2 / 13	0	0	695	370

Évolution depuis le dernier audit

Aucun audit antérieur comparable n'est disponible : l'évolution sera présentée dès le prochain audit.

4 Capacité de remédiation

Ce qui peut réellement être corrigé à la date de l'audit, et par qui. Cette lecture est un **décompte**, pas une note : l'absence de correctif disponible n'est pas une négligence de l'administrateur, mais elle ne diminue pas le risque présent.

SITUATION DU CORRECTIF	QUI PEUT AGIR	TOTAL	CRIT.	ÉLEV.	MOY.	ACTION
Correctif installable depuis les dépôts standard	Administrateur	**0**	0	0	0	Appliquer la mise à jour après sauvegarde et test.
Correctif disponible via Ubuntu Pro (ESM)	Administrateur	**0**	0	0	0	Décider l'activation d'Ubuntu Pro, puis appliquer la mise à jour.
Correctif non encore publié par Ubuntu	Ubuntu	**625**	20	207	225	Surveiller les publications ; limiter l'exposition du service.
Correctif non encore publié par l'éditeur ou le mainteneur	Éditeur / mainteneur	**70**	0	21	41	Surveiller les publications ; évaluer l'isolement ou le retrait.
Vulnérabilités confirmées		**695**				

Hors de ces décomptes

CATÉGORIE	NOMBRE	LECTURE
En attente de qualification par Ubuntu	370	Ni confirmés ni infirmés : aucune remédiation à envisager tant qu'Ubuntu ne s'est pas prononcé.
Paquets obsolètes hors dépôts	0	État non évaluable : à vérifier, puis supprimer ou remplacer.

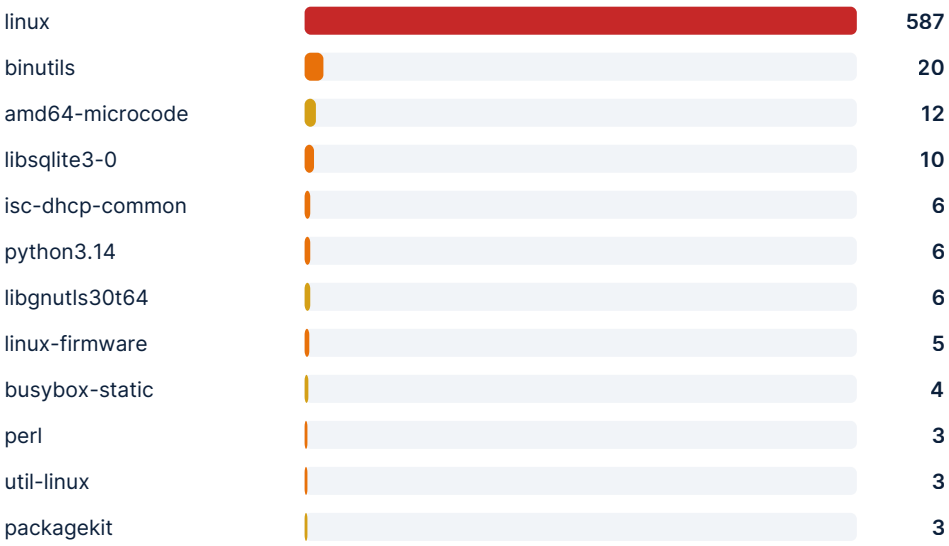
Aucune mise à jour standard n'est à appliquer pour ces failles

Aucune version corrigée n'est publiée dans les dépôts standard pour les vulnérabilités confirmées. L'état de sécurité ne peut donc pas être amélioré par une simple mise à jour.

5 Logiciels les plus concernés

Logiciels cumulant le plus de résultats. Les vulnérabilités **confirmées** et les résultats **en attente de qualification** sont comptés dans des colonnes distinctes : seuls les premiers sont des failles avérées.

Vulnérabilités confirmées par logiciel



Couleur = criticité maximale confirmée du logiciel. Les résultats non confirmés n'apparaissent pas dans ce graphique.

LOGICIEL	CONFIRMÉES	DONT CRIT. / ÉLEVÉES	CRITICITÉ MAXIMALE	EN ATTENTE	SITUATION DU CORRECTIF	MACHINE(S)
linux	587	223	Critique	20	Correctif externe attendu	Serveur 1
binutils	20	3	Élevée	0	Correctif externe attendu	Serveur 1
amd64-microcode	12	0	Moyenne	26	Correctif externe attendu	Serveur 1
libsqlite3-0	10	3	Élevée	0	Correctif externe attendu	Serveur 1
isc-dhcp-common	6	3	Élevée	39	Correctif externe attendu	Serveur 1
python3.14	6	1	Élevée	24	Correctif externe attendu	Serveur 1
libgnutls30t64	6	0	Moyenne	3	Correctif externe attendu	Serveur 1
linux-firmware	5	1	Élevée	39	Correctif externe attendu	Serveur 1

LOGICIEL	CONFIRMÉES	DONT CRIT. / ÉLEVÉES	CRITICITÉ MAXIMALE	EN ATTENTE	SITUATION DU CORRECTIF	MACHINE(S)
busybox-static	4	0	Moyenne	37	Correctif externe attendu	Serveur 1
perl	3	3	Élevée	4	Correctif externe attendu	Serveur 1
util-linux	3	3	Élevée	1	Correctif externe attendu	Serveur 1
packagekit	3	0	Moyenne	2	Correctif externe attendu	Serveur 1

Le détail de chaque CVE figure dans l'analyse des vulnérabilités.

6 Recommandations

Plan d'action hiérarchisé, **serveur par serveur**. Chaque action indique qui peut la réaliser : Client / administrateur pour ce qui est à votre main, Ubuntu / éditeur pour ce qui dépend d'une publication externe.

Serveur 1 — Serveur 1 (OS masque)

Actions immédiates

Aucune action immédiate requise sur ce serveur.

Actions à court terme

- Durcir l'accès SSH selon l'usage réel (clés uniquement, limitation du port, surveillance des tentatives). Client / administrateur

Actions à moyen terme — dépendent d'une publication externe

- Suivre les publications d'Ubuntu et des éditeurs pour 695 failles confirmées en attente de correctif ; documenter l'acceptation du risque ou les mesures compensatoires. Ubuntu / éditeur
- Relancer un audit régulièrement : la distribution confirmera ou écartera les résultats en attente de qualification. Ubuntu / éditeur

Pour l'ensemble des serveurs

Amélioration continue

- Planifier un nouvel audit après chaque campagne de correctifs pour en confirmer l'effet réel. Client / administrateur
- Appliquer régulièrement les mises à jour de sécurité de la distribution. Client / administrateur
- Revoir périodiquement les comptes administrateurs et les ports en écoute. Client / administrateur

Responsabilité

KINLEYAUDIT est un outil de diagnostic : il n'installe, ne modifie ni ne désinstalle jamais rien automatiquement. L'application des correctifs et des mesures de configuration reste sous la responsabilité du client ou de son prestataire. Vérifiez l'avis de sécurité officiel de chaque correctif et testez-le hors production avant application.

7 Méthodologie, limites et glossaire

Sources et méthode

Un agent installé sur chaque serveur audité collecte l'inventaire système (logiciels installés, ports en écoute, pare-feu, configuration SSH, comptes) **sans jamais collecter de mot de passe**. Chaque logiciel est confronté aux sources publiques suivantes :

- **OSV.dev** — base ouverte agrégeant notamment les avis de sécurité Ubuntu/Debian et les CVE.
- **Ubuntu CVE Tracker** (Canonical) — statut officiel par paquet source et par version : confirmé, différé, corrigé, non concerné, ignoré, ou non encore évalué. Ce suivi tient compte des correctifs **rétroportés** par Ubuntu.
- **Index officiels des dépôts Ubuntu** — le paquet existe-t-il encore, et quelle version corrigée est réellement installable.
- **CISA KEV** — catalogue des vulnérabilités activement exploitées dans le monde.
- **Scores CVSS** — calculés selon la formule officielle à partir du vecteur fourni par la source, jamais estimés. Quand plusieurs organismes divergent, tous sont affichés et le score le plus élevé est retenu par prudence.

Une CVE n'est pas comptée comme vulnérabilité simplement parce qu'une base la rattache à une version amont du logiciel : le moteur compare la version installée à la version corrigée selon les règles de versions de la distribution, et s'appuie sur le statut officiel d'Ubuntu. Un paquet dont le numéro semble ancien n'est donc pas considéré comme vulnérable si Ubuntu y a rétroporté le correctif.

Comment lire les deux lectures

- **Note 1 · État de sécurité (A à F)** — mesure le **risque présent**. Départ à 100 ; chaque **logiciel** ayant au moins une faille **confirmée et applicable** retire des points selon sa faille la plus grave, **avec ou sans correctif disponible** : critique 2 points (plafond 30), élevée 0,5 (20), moyenne 0,05 (5), faible 0 ; faille activement exploitée (CISA KEV) 20 (40). Seuils : A ≥ 90, B ≥ 75, C ≥ 60, D ≥ 40, F < 40. Risque : A faible, B/C modéré, D élevé, F critique ; une faille CISA KEV confirmée force « critique ».
- **Note 2 · Hygiène de maintenance (A à F)** — mesure ce qui est **à la main de l'administrateur**. Départ à 100 ; chaque **action** disponible dans les dépôts standard et non appliquée (mise à jour d'un logiciel, ou redémarrage) retire des points selon la faille la plus grave qu'elle corrige : critique 10 (plafond 60), élevée 3 (30), moyenne 0,5 (10). Même échelle de lettres. Ubuntu Pro et les correctifs non publiés ne comptent pas.
- **Ce qui n'entre jamais dans la note** — résultats en attente de qualification, paquets obsolètes hors dépôts, failles déjà corrigées (y compris par rétroportage), non applicables ou ignorées. Ils sont comptés ou listés à part.
- **Ancienne méthode (pour comparaison)** — note unique D (32,0/100) calculée avec l'ancienne formule, moins sévère : elle ne retirait que 2 points par faille critique et ne retenait pas les mêmes plafonds.

Limites de l'analyse et précautions d'interprétation

- Le rapport reflète l'état connu à la date de l'audit ; de nouvelles vulnérabilités sont publiées chaque jour.

- **Gravité théorique et exploitabilité réelle sont deux choses.** Un score CVSS décrit le potentiel d'une faille en général (par exemple « par le réseau, sans authentification ») ; il ne prouve pas qu'elle soit atteignable sur ce serveur. Le rapport distingue l'applicabilité à la version installée (établie par Ubuntu), l'accessibilité du composant (détectée seulement si un service est à l'écoute) et l'exploitation réelle (jamais vérifiée par l'audit).
- La détection repose sur la correspondance entre les logiciels installés et les avis publics. Les avis rattachés à un paquet source dont le nom diffère du paquet installé (par exemple certains composants du noyau) peuvent ne pas être tous couverts ; ce périmètre est en cours d'amélioration, et l'état de sécurité pourrait se dégrader lorsqu'il sera couvert.
- L'exposition réelle depuis Internet n'est pas testée : le pare-feu du fournisseur, un répartiteur de charge ou une règle de traduction d'adresses peuvent la modifier.
- L'agent ne remonte que les services actifs et les processus à l'écoute : il ne peut pas distinguer un service arrêté d'un service absent.
- Un résultat « en attente de qualification » n'est ni confirmé ni infirmé : il ne doit pas être traité comme une faille avérée.
- **Seuls Ubuntu et Debian sont analysés pour les vulnérabilités.** Pour les autres systèmes (Windows, Red Hat…), le rapport présente l'inventaire, les mises à jour en attente et la configuration, **sans note** : l'absence de résultat n'y signifie pas l'absence de vulnérabilité.

Glossaire

CVE
Identifiant public unique d'une vulnérabilité connue (Common Vulnerabilities and Exposures).

CVSS et vecteur CVSS
Score de gravité technique de 0 à 10, et description théorique des conditions d'attaque (réseau ou local, avec ou sans authentification, impact). Ce n'est pas une preuve d'exploitation.

CISA KEV
Catalogue de l'agence américaine CISA des vulnérabilités dont l'exploitation active dans le monde est avérée. L'inscription ne prouve pas que le serveur audité ait été attaqué.

Applicabilité
Une faille est « applicable » lorsqu'Ubuntu confirme qu'elle concerne la version installée du logiciel.

Confirmée / en attente de qualification (needs-triage)
« Confirmée » : la distribution reconnaît que la faille concerne cette version. « En attente de qualification » : la distribution ne s'est pas encore prononcée ; le résultat n'est ni confirmé ni infirmé.

Correctif installable
Une version corrigée est publiée dans les dépôts standard pour la version installée.

Ubuntu Pro (ESM)
Service payant de maintenance de sécurité étendue de Canonical, qui publie des correctifs pour de nombreux logiciels du dépôt « universe » absents des dépôts standard. Son activation est une décision de l'administrateur.

Paquet obsolète (hors dépôts)
Paquet dont la version installée n'est publiée dans aucun dépôt de la version actuelle d'Ubuntu : son état de sécurité ne peut pas être établi.

Paquet source
Nom sous lequel la distribution suit un logiciel, parfois différent de celui du paquet installé.

Correctif rétroporté (backport)
Correctif appliqué par la distribution à une ancienne version d'un logiciel sans en changer le numéro majeur : une version peut être vulnérable en amont et déjà corrigée chez Ubuntu.

Écoute, règle UFW, exposition Internet
« Écoute » : un processus attend des connexions sur un port. « Règle UFW » : le pare-feu du serveur autorise explicitement ce port. « Exposition Internet » : le port est réellement joignable depuis Internet, ce que seul un test externe peut établir.

Annexe A — Sources et références

- **OSV.dev** — `https://osv.dev` · API : `https://api.osv.dev/v1/vulns/<identifiant>`
- **Ubuntu CVE Tracker** — `https://ubuntu.com/security/cves` et dépôt `ubuntu-cve-tracker` de Canonical.
- **Dépôts Ubuntu** — `http://archive.ubuntu.com/ubuntu` et `http://security.ubuntu.com/ubuntu` (index des paquets).
- **CISA KEV** — `https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
- **CVSS** — `https://www.first.org/cvss/`

Rapport généré automatiquement par KINLEYAUDIT pour KINLEY MARKETING SECURITY — 27/11/2026 à 13:49 (heure de Paris). Exemple de rapport, données anonymisées.