5 ANALYSES STATISTIQUES DES CVEs LIÉES AUX VULNÉRABILITÉS ReDoS :

Cette 5e partie présente une étude empirique des failles de sécurité liées aux attaques ReDoS, à partir des caractéristiques CVSS des CVEs identifiées. L'objectif est de dégager les tendances générales, les niveaux de gravité prédominants, ainsi que les conditions d'exploitation (vecteur d'attaque, interaction requise, privilèges) les plus fréquemment associées à ces vulnérabilités. Les caractéristiques analysées comprennent notamment :

- Le vecteur d'attaque (attackVector) : *NETWORK*, *ADJACENT NETWORK*, *LOCAL*, *PHYSICAL*
- La complexité d'attaque (attackComplexity) : *LOW*, *HIGH*
- Les privilèges requis (privilegesRequired) : *NONE*, *LOW*, *HIGH*
- L'interaction utilisateur (userInteraction) : *NONE*, *REQUIRED*
- La gravité de base (baseSeverity) : *LOW*, *MEDIUM*, *HIGH*
- Les scores numériques :
    - baseScore (score global)
    - exploitabilityScore (facilité d'exploitation)
    - impactScore (impact potentiel)

Des analyses croisées ont également été menées pour étudier l'impact combiné de certaines caractéristiques sur la sévérité des vulnérabilités.

Analyse univariée des caractéristiques CVSS :

Cette première sous-section présente l'analyse univariée de chaque caractéristique issue des métadonnées CVSS. Elle permet d'identifier les distributions des vecteurs d'attaque, de complexité, de privilèges, etc., afin de mieux comprendre le profil général des vulnérabilités ReDoS recensées.

Distribution des vecteurs d'attaque :

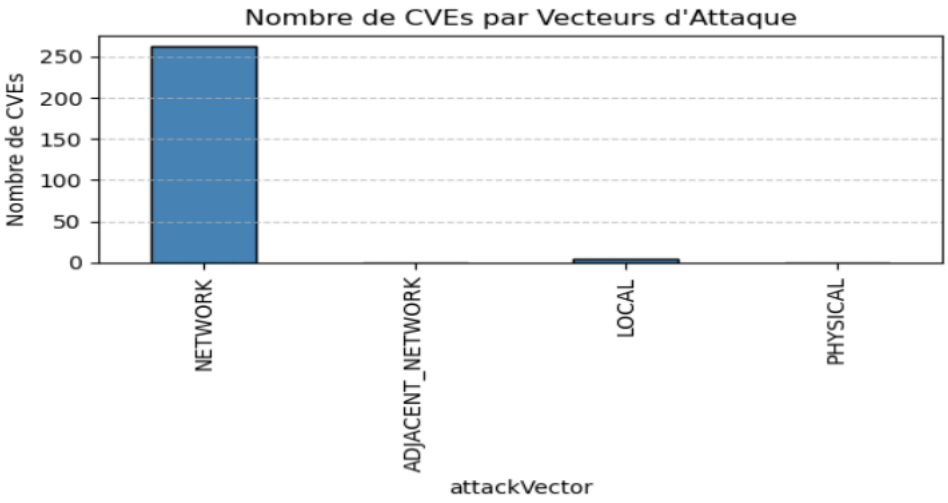

Figure 36 : Distribution des CVEs ReDoS selon le vecteur d'attaque CVSS.

Le vecteur d'attaque majoritaire pour les vulnérabilités ReDoS est *NETWORK*, ce qui signifie que la grande majorité des attaques identifiées peuvent être déclenchées à distance, via des communications réseau. Cela accentue le niveau de criticité de ces vulnérabilités dans des contextes de déploiement web ou d'API accessibles publiquement. Les autres vecteurs (*LOCAL*, *ADJACENT_NETWORK*, *PHYSICAL*) sont quasi inexistants, ce qui suggère que ReDoS est principalement une menace réseau. À noter également la présence d'un nombre significatif de valeurs nulles, indiquant une incomplétude des données CVSS pour certaines CVEs.

Distribution des CVEs selon la complexité d'attaque :

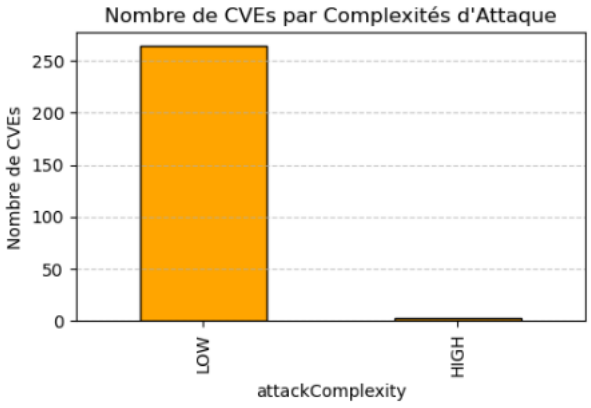

Figure 37 : Distribution des CVEs ReDoS selon la complexité d'attaque CVSS.

La répartition des CVEs selon la complexité d'attaque montre une nette prédominance des attaques à faible complexité (*LOW*). Cela signifie que l'exploitation des vulnérabilités ReDoS identifiées ne requiert généralement aucune condition technique contraignante. Seules quelques CVEs impliquent une complexité plus élevée (*HIGH*), rendant leur exploitation plus difficile. Alors, la tendance globale est claire : les attaques ReDoS sont majoritairement simples à exécuter, ce qui en fait un vecteur d'attaque préoccupant, même pour des acteurs peu qualifiés.

Distribution des CVEs par Privilèges Requis :

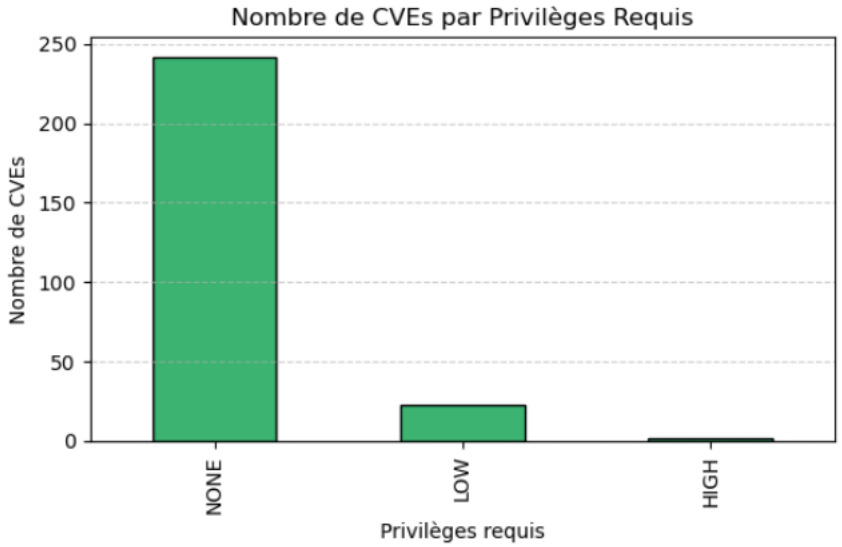

Figure 38 : Distribution des CVEs ReDoS selon les privilèges requis (métriques CVSS.)

La majorité des vulnérabilités ReDoS répertoriées peuvent être exploitées sans aucun privilège préalable (*NONE*). Cela traduit une accessibilité critique de ces attaques, car un utilisateur lambda ou un acteur non authentifié pourrait déclencher une défaillance du système via des expressions régulières mal sécurisées. Quelques CVEs nécessitent des privilèges faibles (*LOW*), et très peu exigent des privilèges élevés (*HIGH*), ce qui corrobore la nature largement exploitable des ReDoS.

Distribution des CVEs par Intéraction d'Utilisateur :

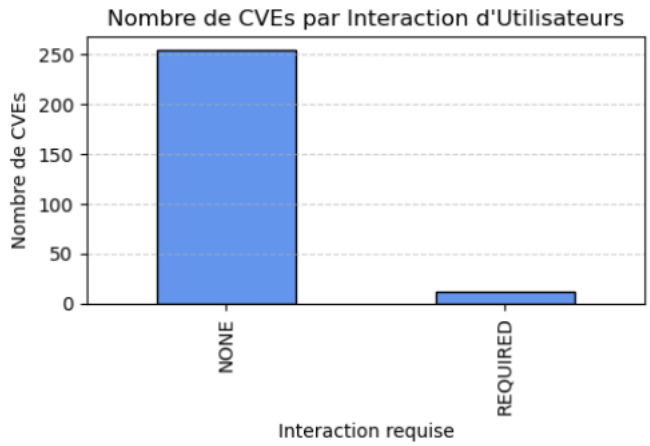

Figure 39 : Distribution des CVEs ReDoS selon l'interaction requise avec l'utilisateur.

La très grande majorité des CVEs recensées dans les vulnérabilités ReDoS ne nécessitent aucune interaction humaine (*NONE*) pour être exploitées. Cela signifie que l'attaque peut être déclenchée automatiquement via un appel HTTP, une soumission de formulaire, ou tout autre traitement automatisé de l'entrée utilisateur. Très peu d'expressions nécessitent une interaction explicite (*REQUIRED*), comme un clic ou une action manuelle, ce qui montre que les vulnérabilités ReDoS sont hautement exploitables dans des environnements automatisés ou serveurs back-end.

Distribution des CVEs par Sévérité :

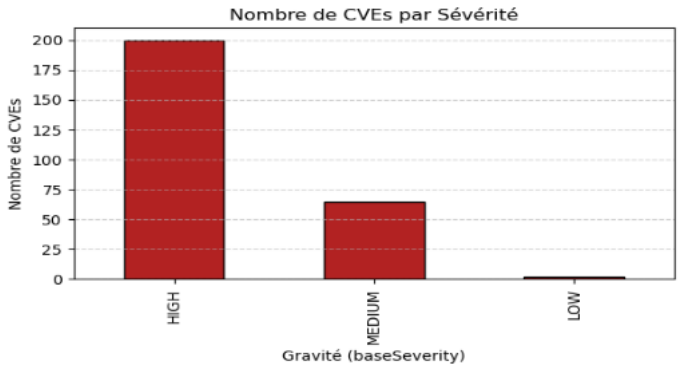

Figure 40 : Distribution des CVEs ReDoS selon le niveau de sévérité (baseSeverity CVSS.)

Le graphe montre que la majorité des vulnérabilités ReDoS recensées sont classées à haute sévérité (*HIGH*), avec environ 200 CVEs. Cela reflète leur capacité à engendrer des dénis de service critiques pouvant impacter gravement la disponibilité des systèmes. Les niveaux (*MEDIUM)* sont représentés, suggérant des vulnérabilités à impact plus limité ou contextuel. Le faible nombre de CVEs classées (*LOW)* indique que les vulnérabilités ReDoS sont rarement considérées bénignes.

Distribution des CVEs par baseScore :

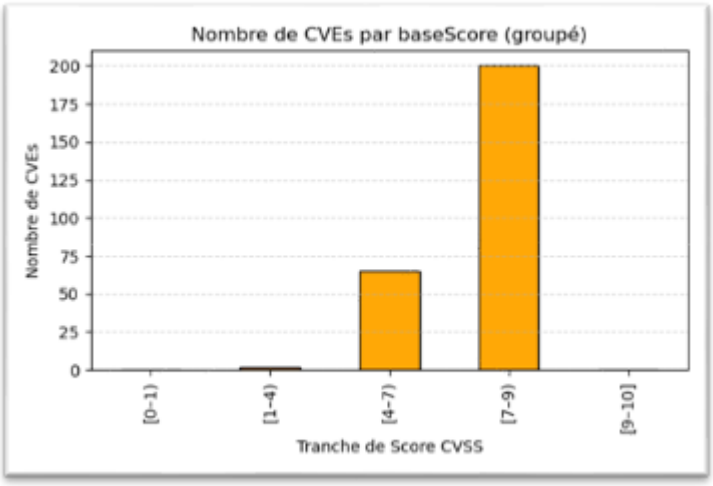

Figure 41 : Distribution des CVEs ReDoS selon les tranches de score CVSS de base (baseScore groupé.)

Le baseScore, noté sur 10, quantifie l'intensité d'une vulnérabilité selon le système CVSS. Le regroupement des scores montre :

- Une forte concentration dans l'intervalle [7–9), représentant près de la moitié des CVEs. Cela confirme que la majorité des vulnérabilités ReDoS sont jugées sévères.
- L'intervalle [4–7) regroupe un volume modéré, associé aux vulnérabilités de gravité moyenne.
- Très peu de CVEs se situent sous [4[, ce qui montre que les ReDoS sont rarement considérées comme bénignes.

Répartition des CVEs par Scores d'Exploitabilité :

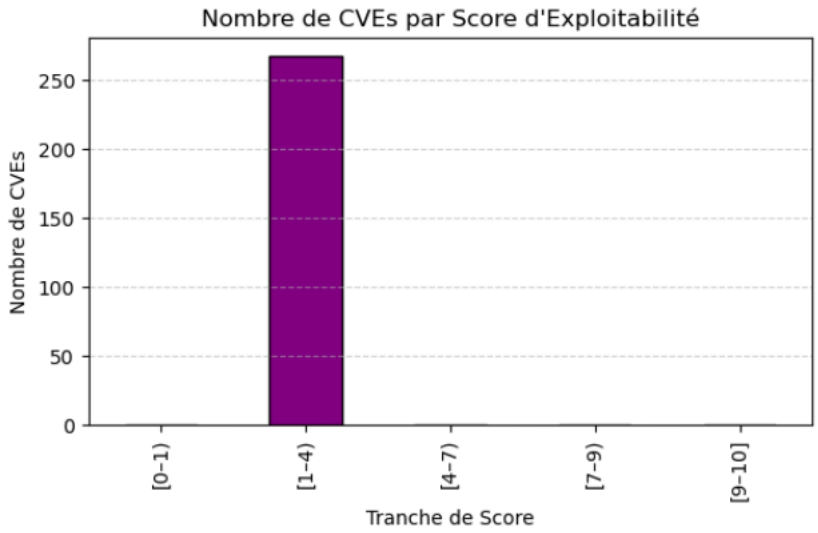

Figure 42 : Répartition des CVEs ReDoS selon la tranche de score d'exploitabilité CVSS.

Le Score d'Exploitabilité quantifie la facilité avec laquelle une vulnérabilité peut être exploitée. Les résultats montrent :

- La quasi-totalité des CVEs se situe dans l'intervalle [1–4).
- Aucune vulnérabilité n'atteint les tranches supérieures [4–7) ou [7–10).
- Environ 50 CVEs sont non renseignées (null).

Cela montre que :

- Les vulnérabilités ReDoS sont relativement faciles à exploiter, mais peu atteignent un niveau de complexité très bas (score proche de 0).
- Les scores sont modérés, indiquant que l'exploitation ne nécessite pas de compétences avancées, mais n'est pas totalement triviale non plus.

Répartition des CVEs par Scores d'Impact :

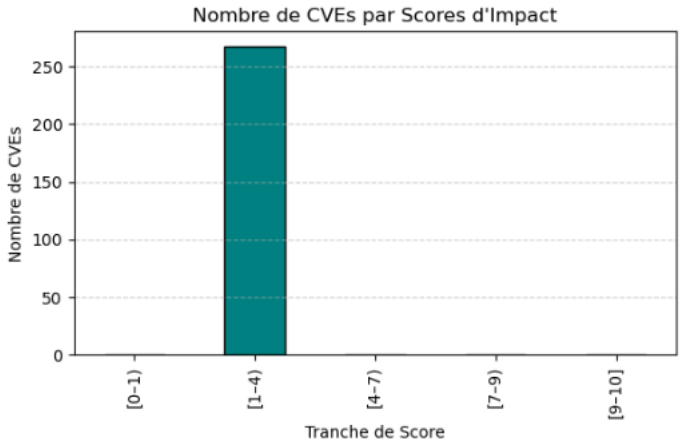

Figure 43 : Répartition des CVEs ReDoS selon la tranche de score d'impact CVSS.

Ce score mesure les conséquences potentielles d'une exploitation réussie, notamment sur la confidentialité, l'intégrité et la disponibilité. Les résultats observés sont les suivants :

- La majorité écrasante des CVEs se trouve dans la tranche [1–4).
- Aucune vulnérabilité n'atteint des niveaux d'impact modéré ou élevé (aucun dans les tranches [4–7), [7–9), [9–10]).

Bien que les vulnérabilités ReDoS soient fréquentes et faciles à déclencher, leur impact reste généralement faible à modéré. Cela peut s'expliquer par le fait qu'elles entraînent des ralentissements ou blocages de services, sans compromettre directement des données sensibles. Le manque de CVEs dans les tranches élevées confirme que ReDoS est surtout un risque de disponibilité plutôt qu'un vecteur de compromission critique.

Analyses croisées :

Après avoir examiné individuellement chaque caractéristique des CVEs, nous poursuivons avec une analyse croisée visant à explorer les relations entre deux dimensions combinées. Ces croisements permettent de mieux comprendre l'interaction entre les facteurs de risque (comme l'origine de l'attaque et sa gravité, ou les exigences d'accès et d'interaction humaine), et d'en dégager des profils types de vulnérabilités ReDoS.

Les croisements étudiés porteront notamment sur :

- Vecteurs d'attaque × Sévérité
- Privilèges requis × Interaction utilisateur
- Sévérité × Scores d'exploitabilité
- Sévérité × Scores d'impact

Vecteurs d'attaque × Sévérité :

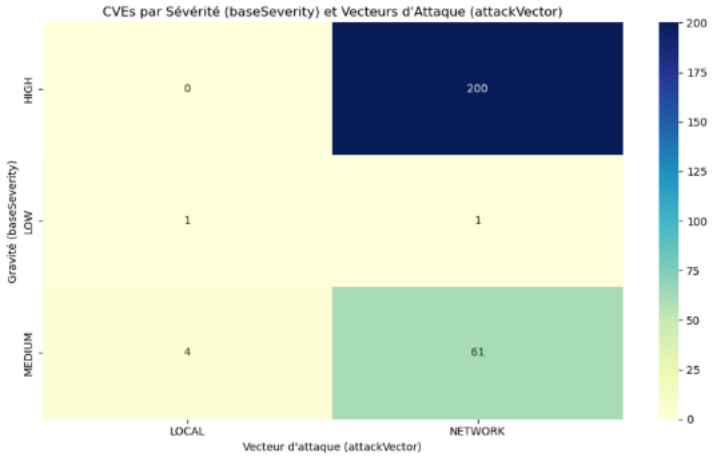

Figure 44 : Croisement des CVEs ReDoS selon la gravité (baseSeverity) et le vecteur d'attaque (attackVector.)

Le graphique de chaleur ci-dessus met en évidence l'analyse croisée entre les Vecteur d'attaque (attackVector) et la Sévérité (baseSeverity). Les vulnérabilités de sévérité élevée (*HIGH*) sont majoritairement associées au vecteur *NETWORK*. Puis les CVEs de gravité moyenne (*MEDIUM*) sont également surtout liées à *NETWORK*, mais quelques cas concernent le vecteur *LOCAL*. Les attaques ReDoS les plus graves sont typiquement accessibles via le réseau, ce qui accentue leur potentiel de nuisance.
Cela souligne l'importance de prioriser la surveillance réseau et l'analyse des expressions exposées en ligne.

Privilèges requis × Interaction utilisateur :

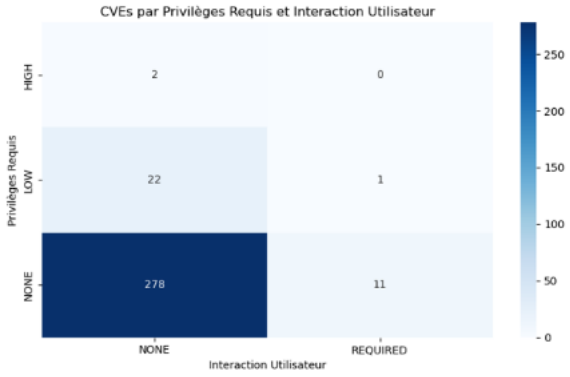

Figure 45 : Croisement des CVEs ReDoS selon les privilèges requis et l'interaction utilisateur.

Ce deuxième graphique croisé examine la relation entre les Privilèges requis (privilegesRequired) et les interactions utilisateurs (userInteraction). D'après la figure, Une très large majorité des CVEs

(231) n'exigent aucun privilège et aucune interaction : ce sont les plus accessibles. Les combinaisons impliquant une interaction utilisateur sont rares (seulement 12 CVEs au total). Les cas où les deux champs sont None (manquants) sont également bien identifiés (47 cas). La vulnérabilité des expressions ReDoS repose massivement sur leur accessibilité directe, sans barrière d'authentification ou d'action manuelle. Cela montre leur danger potentiel en production, surtout dans les services web.

Sévérité × Scores d'exploitabilité :

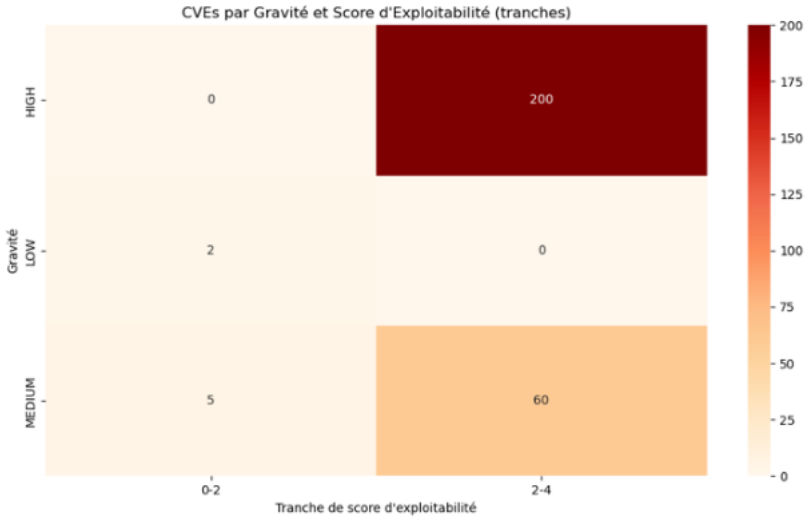

Figure 46 : Répartition des CVEs ReDoS selon la gravité (baseSeverity) et le score d'exploitabilité (groupé).

Cette troisième analyse croisée explore le lien entre La sévérité des vulnérabilités (baseSeverity) et leur Exploitabilité (exploitabilityScoreRange) regroupée en deux tranches : 0–2 (faible) et 2–4 (modérée). Il apparaît clairement que plus la gravité est élevée, plus l'exploitabilité reste modérée mais suffisante. Cela montre que les failles ReDoS, bien que techniquement simples, ont un fort potentiel d'exploitation, justifiant leur sévérité.

Sévérité × Scores d'impact :

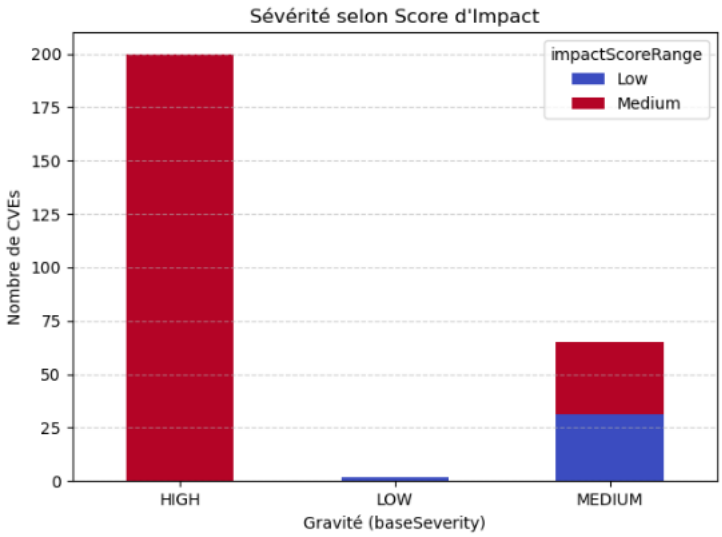

Figure 47 : Distribution des CVEs ReDoS selon la gravité (baseSeverity) et les tranches du score d'impact.

Comprendre si le niveau de gravité attribué aux vulnérabilités est bien corrélé à leur impact réel (mesuré via impactScore). On observe que Toutes les CVEs sévères (*HIGH*) sont associées à un impact moyen, ce qui confirme une certaine cohérence dans l'évaluation. Les vulnérabilités moyennes (*MEDIUM*) montrent une répartition équilibrée entre impact faible et moyen. Une seule CVE de faible gravité (*LOW*) a un impact faible. On peut conclure que l'évaluation de la gravité est généralement alignée avec l'impact mesuré, ce qui crédibilise les scores CVSS. Cela montre aussi que les vulnérabilités ReDoS, même si leur mécanisme est simple, ont un impact assez significatif.

Analyse temporelle des CVEs ReDoS publiées :

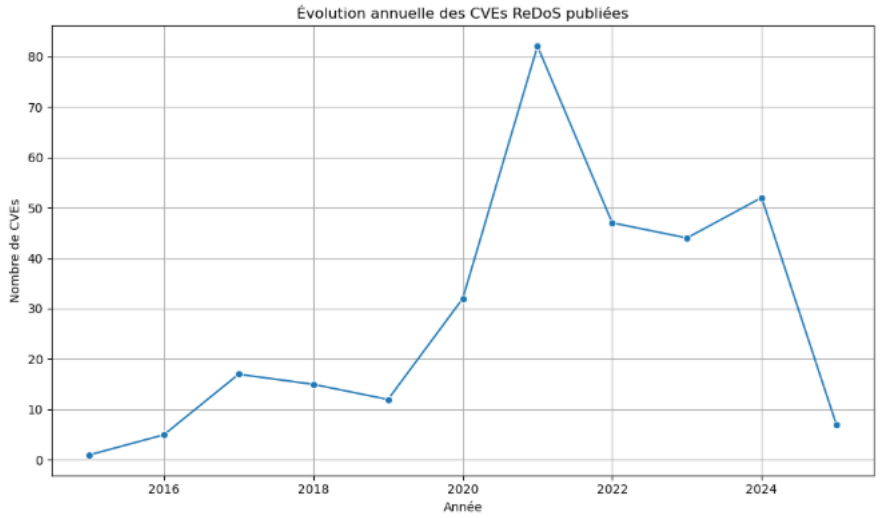

Figure 48 : Évolution temporelle des vulnérabilités ReDoS référencées dans la base CVE (2015–2025).

L'analyse de la courbe annuelle des CVEs liées aux vulnérabilités ReDoS révèle une progression structurée en plusieurs phases. Entre 2015 et 2019, les publications sont rares, témoignant d'une faible sensibilisation au risque ReDoS ou de l'absence d'outils de détection efficaces. Un tournant s'opère à partir de 2019, plus accentué en 2020, avec une forte hausse des publications qui atteint un pic historique en 2021 avec plus de 80 CVEs. Cette explosion s'explique non seulement par l'intégration croissante d'outils automatisés de détection dans les pipelines DevSecOps, mais aussi par un contexte mondial particulier :

- La pandémie de COVID-19 a entraîné une accélération de la numérisation, une augmentation de la surface d'attaque, et un usage massif de composants open source, favorisant la détection de vulnérabilités comme le ReDoS.
- La montée en puissance des audits de sécurité sur les bibliothèques JavaScript, Python et autres a contribué à mettre en lumière des patterns jusque-là négligés. [16][17][18] souligne que 80 % des organisations compilent du code quotidiennement ou hebdomadairement, seulement 27 % réalisent des audits de sécurité continuels. Par ailleurs, depuis 2021, plusieurs travaux académiques et outils ont émergé pour détecter automatiquement les vulnérabilités ReDoS dans les expressions régulières et leur adoption a permis d'identifier des modèles vulnérables qui n'avaient pas été repérés par des approches plus classiques [19][20][21].

La période 2022–2024 traduit une forme de régulation autour de 45–52 CVEs par an. Ce plateau pourrait indiquer un équilibre entre détection proactive et durcissement des pratiques de développement sécurisé.

Enfin, la chute marquée en 2025 (8 CVEs) est à relativiser, car l'année n'est pas encore écoulée, et les CVEs continuent d'être traitées avec un décalage temporel (publication post-audit ou post-mitigation).