Engineer

CVE

liste publique donnant un identifiant par faille divulguée

Ce que c’est

CVE, abréviation de Common Vulnerabilities and Exposures, est le catalogue public des vulnérabilités de cybersécurité divulguées publiquement, avec une fiche CVE pour chacune. Le CVE Program décrit sa mission comme l’identification, la définition et le catalogage de ces vulnérabilités, afin que deux personnes ou deux outils puissent désigner une faille en sachant qu’ils parlent de la même. Le mot désigne le programme, la liste et, de manière moins stricte, une entrée, comme dans « cette bibliothèque a deux CVE non résolues ».

Chaque fiche porte un identifiant CVE. Son format est le préfixe `CVE`, une année à quatre chiffres et un numéro séquentiel de quatre chiffres ou plus. `CVE-1999-0067`, `CVE-2019-12345` et `CVE-2021-7654321` sont donc tous valides ; le programme ne fixe aucune limite supérieure à la longueur du numéro. L’année est celle de la réservation de l’identifiant ou de la publication de la vulnérabilité. Selon les termes du programme, « la composante année ne sert pas à indiquer quand la vulnérabilité a été découverte ».

Les identifiants ne sont pas distribués par un guichet central unique. Les CVE Numbering Authorities, ou CNA, sont des fournisseurs, des chercheurs, des projets libres, des équipes de réponse aux incidents, des opérateurs de services en ligne, des prestataires de primes aux bogues et des consortiums autorisés par le programme à attribuer des identifiants et publier des fiches, chacun dans son périmètre. Toute fiche CVE est ajoutée par une CNA. Devenir CNA ne demande ni frais ni contrat à signer, et le programme en accueille activement de nouvelles depuis 2016.

Une fiche passe par trois états. Elle commence à l’état Reserved (« réservé »), lorsqu’une CNA a réservé un identifiant que les parties utilisent pour coordonner les premiers travaux sur la vulnérabilité avant divulgation. Elle passe à l’état

Published (« publié »), quand la CNA a renseigné au moins l'identifiant, une courte description, les produits et versions concernés et une référence publique. Si l'identifiant ne doit plus être utilisé, elle passe à l'état Rejected (« rejeté »), et reste dans la liste pour que quiconque le possède voie qu'il est invalide.

L'idée remonte à 1999. Deux ingénieurs de MITRE, David E. Mann et Steven M. Christey, l'ont présentée dans un livre blanc lors d'un atelier à Purdue University en janvier 1999. La liste a été rendue publique en septembre 1999 avec 321 fiches.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce que CVE ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Des comptes, mots de passe et droits attribués selon les besoins exacts de chaque poste, puis retirés le jour du départ.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 1 000 règles RBAC pour sécuriser Linux — 1,000 règles d'accès écrites pour combler une faille de sécurité

1 000 règles RBAC pour sécuriser Linux Contactez-nous →

Pourquoi c'est important

Un rapport de vulnérabilité n'est utile que si ses lecteurs peuvent déterminer s'il décrit le même problème qu'un autre rapport. L'identifiant CVE tranche : deux avis, un résultat de scanner et un ticket portant le même identifiant concernent la même faille. De nombreux grands fournisseurs de systèmes d'exploitation mettent les identifiants CVE dans leurs avis pour que tous les aient dès l'annonce. Les produits et services de sécurité du monde entier intègrent les fiches CVE à leurs rapports.

D'autres services se construisent sur la liste plutôt qu'à côté d'elle. La National Vulnerability Database des États-Unis, lancée par le NIST en 2005, est un programme distinct qui s'appuie sur les fiches CVE et ajoute son analyse à chacune. Le catalogue Known Exploited Vulnerabilities, ou KEV, de CISA recense des failles dont l'exploitation par des attaquants a été observée. Chaque entrée indique l'identifiant CVE et renvoie à sa fiche.

Ce qu'il est le plus utile de savoir sur CVE, c'est ce qu'il ne représente pas. La gravité se mesure séparément avec CVSS, le Common Vulnerability Scoring System, une norme gérée par FIRST, organisation sans but lucratif établie aux États-Unis qui aide les équipes de réponse aux incidents de sécurité informatique

du monde entier. CVSS 4.0 note une vulnérabilité de 0 à 10 à l'aide des groupes de métriques de base, de menace, environnementales et complémentaires. Il associe le nombre aux niveaux de gravité nulle, faible, moyenne, élevée et critique, ce dernier allant de 9,0 à 10,0. Le CVE Record Format permet à une CNA d'inclure un score CVSS dans sa fiche, mais ce score appartient à CVSS, pas à l'identifiant : une même faille peut avoir plusieurs scores de sources différentes, ou aucun.

Ce n'est pas non plus une classe de faiblesse. La Common Weakness Enumeration, CWE, est une liste communautaire de faiblesses : des conditions présentes dans un logiciel, un micrologiciel, du matériel ou un service qui peuvent, dans les bonnes circonstances, laisser apparaître une vulnérabilité. Le CVE Program présente les CWE comme les causes fondamentales des fiches CVE. Une CVE nomme une faille dans un produit ; une CWE nomme le type d'erreur qui l'explique. L'injection SQL, par exemple, est la faiblesse CWE-89, et chaque produit où cette erreur est trouvée reçoit son propre identifiant CVE.

À quoi cela ressemble en pratique

Shellshock, la faille de Bash de 2014, montre les trois systèmes côte à côte. cve.org affiche les fiches dans le CVE Record Format, un format JSON. Le début de celle-ci est le suivant, avec des champs omis et réordonnés :


```
{
  "dataType": "CVE_RECORD",
  "dataVersion": "5.1",
  "cveMetadata": {
    "cveId": "CVE-2014-6271",
    "assignerShortName": "debian",
    "state": "PUBLISHED",
    "dateReserved": "2014-09-09T00:00:00.000Z",
    "datePublished": "2014-09-24T18:00:00.000Z",
    "dateUpdated": "2025-10-22T00:05:36.342Z"
  }
}
```


Debian, en qualité de CNA, a réservé l'identifiant le 9 septembre 2014 et publié la fiche quinze jours plus tard. La description dit que Bash jusqu'à la version 4.3 traite le texte suivant une définition de fonction dans la valeur d'une variable d'environnement. Un attaquant distant peut ainsi exécuter du code arbitraire au moyen d'un environnement spécialement construit. Elle précise aussi que le

premier correctif était erroné et que la partie de la faille que ce correctif n'avait pas éliminée a reçu son propre identifiant, CVE-2014-7169. Les équipes qui avaient appliqué un correctif puis s'étaient arrêtées restaient exposées.

La fiche contient ensuite des conteneurs de trois sources différentes. Le conteneur CNA porte la description et les références de Debian. Le CVE Program Container ajoute ses propres références. Un troisième, provenant d'un Authorized Data Publisher et intitulé CISA ADP Vulnrichment, ajoute ce que l'identifiant CVE seul ne contient pas :

```
{
  "cvssV3_1": {
    "version": "3.1",
    "vectorString": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H",
    "baseScore": 9.8,
    "baseSeverity": "CRITICAL"
  }
}
```

La chaîne qui décrit le vecteur détaille les raisons du score de 9,8 : une attaque par le réseau, de faible complexité, sans privilèges ni interaction utilisateur, avec un impact élevé sur la confidentialité, l'intégrité et la disponibilité. Le même conteneur rattache la faille à CWE-78, la classe de faiblesse des injections de commandes du système d'exploitation, et note que CISA l'a ajoutée au catalogue KEV le 28 janvier 2022. Une seule fiche contient donc un identifiant du CVE Program, un score d'une version de CVSS publiée par FIRST et une classe de faiblesse de CWE, chacun d'une source différente et répondant à une question différente.

Au quotidien, les identifiants CVE servent surtout de clés, plutôt que de contenu à lire. Notre page de sécurité décrit la routine : les composants de chaque système sont inventoriés, puis leur liste est comparée aux avis publiés, au lieu de tenir ces composants pour fiables sous prétexte qu'ils fonctionnaient auparavant. L'identifiant CVE permet de remonter d'un résultat de ce contrôle à l'avis, puis de suivre le chemin jusqu'à la mise à niveau qui le résout.

Où les problèmes surviennent

On lit le score comme le risque. Si personne ne fournit les valeurs de menace ou environnementales, la spécification CVSS 4.0 les remplit avec des valeurs par défaut supposant le pire. Elle note aussi que NVD et les mainteneurs de produits ne publient généralement que le score de base. Un 9,8 sur un composant inaccessible de l'extérieur n'est pas un 9,8 pour vous. Étiquetez les scores comme le demande la spécification : CVSS-B pour la base seule et CVSS-BTE lorsque les valeurs de menace et environnementales ont été appliquées. Ajoutez les valeurs environnementales de vos systèmes avant de définir les priorités du travail.

CVE, CVSS et CWE sont confondus. « Une CVE de 9,8 » mélange identifiant et score ; « la CVE d'injection SQL » mélange une faille et une classe de failles. Distinguez les trois dans les tickets et rapports : l'identifiant de CVE, le score avec sa version de CVSS et la cause fondamentale de CWE.

On cite le nombre sans son vecteur. FIRST exige de toute personne publiant des données CVSS qu'elle publie leur vecteur avec le nombre, pour rendre les choix sous-jacents vérifiables. Un nombre seul ne peut être vérifié, comparé entre versions de CVSS ou ajusté à votre contexte. Conservez le vecteur complet, dont le préfixe `CVSS:3.1/` ou `CVSS:4.0/` qui indique la version.

On prend l'année pour la date de découverte. L'année de l'identifiant est celle de sa réservation ou de la divulgation de la faille. Un identifiant de 2014 peut décrire du code livré dans les années 1990, et une faille trouvée en décembre peut porter le numéro de l'année suivante. Pour les dates, utilisez les champs `dateReserved` et `datePublished` de la fiche, jamais l'identifiant.

On suppose quatre chiffres. Le numéro séquentiel comporte au moins quatre chiffres, sans limite supérieure ; une expression comme `CVE-\d{4}-\d{4}` tronque donc silencieusement les identifiants plus longs. Utilisez plutôt `^CVE-[0-9]{4}-[0-9]{4,}$` et traitez l'identifiant comme une chaîne, pas comme un nombre, pour garder les zéros initiaux.

On traite une fiche rejetée comme absente. Un identifiant Rejected reste volontairement dans la liste pour signaler son invalidité. Un outil qui l'ignore, ou le compte comme un problème ouvert, induit en erreur dans l'un ou l'autre sens. Lisez le champ `state` et traitez explicitement `REJECTED` .

On considère la fiche comme définitive. La dernière modification de la fiche Shellshock date d'octobre 2025, onze ans après publication, et son entrée KEV de janvier 2022. La spécification CVSS utilise son groupe de menace pour prendre en compte l'évolution du contexte d'une vulnérabilité. Relisez les fiches correspondant à chaque problème dont vous avez accepté le risque plutôt que de le corriger, selon un calendrier établi.

On s'arrête au premier correctif. Shellshock a nécessité un second identifiant parce que le premier correctif laissait une partie de la faille ouverte. Lisez la description et les références de chaque fiche pour repérer les identifiants de suivi, puis ne fermez le problème que lorsque tous les identifiants qui désignent le composant sont résolus.

On assimile absence de CVE et absence de vulnérabilité. CVE couvre les vulnérabilités divulguées publiquement et identifiées par une CNA dans son périmètre. Une faille de votre code n'a pas de CVE tant que personne ne l'a signalée et publiée. Comparer les dépendances à la liste couvre ce que d'autres ont trouvé ; votre code a besoin de sa propre analyse statique, de revues et de tests.

Pour aller plus loin

- CVE Program : présentation — la mission, la fiche CVE et les partenaires qui attribuent les identifiants et publient les fiches.
- CVE Program : processus — le format de l'identifiant, le contenu minimal d'une fiche et ses trois états.
- CVE Program : démarches associées — les liens de NVD, CVSS, du catalogue KEV et de CWE avec CVE, et leurs différences.
- Common Vulnerability Scoring System v4.0 : spécification — les groupes de métriques, les étiquettes de score et l'échelle qualitative de gravité de FIRST.

- CVE Record Format — la définition JSON de la structure d’une fiche, dans la version utilisée par CVE Services.

- CVE Program : questions fréquentes (archives)

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce que CVE ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/cve/