Engineer

CVE

öffentliche Liste: eine ID je offengelegter Schwachstelle

Was es ist

CVE, kurz für Common Vulnerabilities and Exposures, ist der öffentliche Katalog öffentlich bekannt gemachter Cybersicherheitsschwachstellen mit einem CVE Record für jede davon. Das CVE Program beschreibt seine Aufgabe als Identifizieren, Definieren und Katalogisieren dieser Schwachstellen. So können zwei Personen oder zwei Werkzeuge auf einen Fehler verweisen und wissen, dass sie denselben meinen. Der Begriff bezeichnet das Programm, die Liste und im lockeren Gebrauch auch einen einzelnen Eintrag, etwa in „Diese Bibliothek hat zwei offene CVEs“.

Jeder Eintrag trägt eine CVE-ID. Ihr Format besteht aus dem Präfix `CVE`, einer vierstelligen Jahreszahl und einer Folgenummer mit vier oder mehr Ziffern. `CVE-1999-0067`, `CVE-2019-12345` und `CVE-2021-7654321` sind also alle gültig. Das Programm legt keine Obergrenze für die Länge der Folgenummer fest. Die Jahreszahl bezeichnet das Jahr, in dem die ID reserviert oder die Schwachstelle veröffentlicht wurde. Das Programm formuliert es so: „Der Jahresanteil gibt nicht an, wann die Schwachstelle entdeckt wurde.“

IDs werden nicht von einer einzigen zentralen Stelle vergeben. CVE Numbering Authorities, kurz CNAs, sind Hersteller, Forscher, Open-Source-Projekte, Notfallteams, Betreiber von Onlinediensten, Bug-Bounty-Anbieter und Konsortien, die das Programm zur Vergabe von IDs und zur Veröffentlichung von Einträgen ermächtigt hat, jeweils innerhalb ihres eigenen Zuständigkeitsbereichs. Jeder CVE Record wird von einer CNA hinzugefügt. Um CNA zu werden, muss man weder eine Gebühr zahlen noch einen Vertrag unterzeichnen. Seit 2016 baut das Programm ihre Zahl aktiv aus.

Ein Eintrag durchläuft drei Zustände. Er beginnt als Reserved, wenn eine CNA eine ID reserviert hat, mit der die Beteiligten ihre frühe Arbeit an der Schwachstelle vor der Offenlegung abstimmen. Er wird Published, sobald die CNA mindestens die ID, eine kurze Beschreibung, die betroffenen Produkte und Versionen sowie eine öffentliche Referenz eingetragen hat. Soll die ID nicht mehr verwendet werden, wird sie Rejected. Der Eintrag bleibt auf der Liste, damit jeder mit dieser ID sehen kann, dass sie ungültig ist.

Die Idee stammt aus dem Jahr 1999. Zwei MITRE-Ingenieure, David E. Mann und Steven M. Christey, stellten das Konzept im Januar 1999 bei einem Workshop an der Purdue University als Whitepaper vor. Im September 1999 wurde die Liste mit 321 Einträgen veröffentlicht.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist CVE?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. Konten, Passwörter und Berechtigungen werden so geordnet, dass alle genau den beruflich erforderlichen Zugriff haben und ihn am Tag ihres Ausscheidens verlieren.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 1.000 RBAC-Regeln für sichere Linux-Server — 1,000 Zugriffsregeln zum Schließen einer Sicherheitslücke

1.000 RBAC-Regeln für sichere Linux-Server Kontakt aufnehmen →

Warum es wichtig ist

Ein Schwachstellenbericht ist nur nützlich, wenn Leser erkennen können, ob er dasselbe Problem behandelt wie ein anderer Bericht. Eine CVE-ID klärt das: Zwei Sicherheitshinweise, ein Scannerbefund und ein Ticket mit derselben ID betreffen denselben Fehler. Zahlreiche große Betriebssystemanbieter nehmen CVE-IDs in ihre Sicherheitshinweise auf, damit die ID allen ab der Bekanntgabe eines Problems zur Verfügung steht. Sicherheitsprodukte und -dienste weltweit integrieren CVE Records in ihre Meldungen.

Andere Dienste bauen auf der Liste auf, statt neben ihr zu stehen. Die US-amerikanische National Vulnerability Database, die NIST 2005 startete, ist ein eigenständiges Programm. Sie baut auf CVE Records auf und ergänzt jeden um ihre eigene Analyse. Der Katalog Known Exploited Vulnerabilities (KEV) von CISA führt Fehler auf, deren tatsächliche Ausnutzung durch Angreifer beobachtet wurde. Jeder Eintrag nennt seine CVE-ID und verlinkt den zugehörigen Datensatz.

Am nützlichsten ist es, CVE von den benachbarten Begriffen abzugrenzen. Der Schweregrad wird getrennt mit CVSS, dem Common Vulnerability Scoring System, gemessen. Diesen Standard betreut FIRST, eine gemeinnützige Organisation mit Sitz in den USA, deren Aufgabe die Unterstützung von Teams für die Reaktion auf IT-Sicherheitsvorfälle weltweit ist. CVSS Version 4.0 bewertet eine Schwachstelle anhand der Metrikgruppen Base, Threat, Environmental und Supplemental auf einer Skala von 0 bis 10. Die Zahl wird den Stufen None, Low, Medium, High und Critical zugeordnet. Critical reicht von 9,0 bis 10,0. Das CVE Record Format erlaubt einer CNA, einen CVSS-Wert in ihren Eintrag aufzunehmen. Der Wert gehört aber zu CVSS, nicht zur ID: Ein Fehler kann verschiedene Bewertungen verschiedener Herausgeber haben oder gar keine.

Ebenso wenig ist CVE eine Schwächenklasse. Die Common Weakness Enumeration, CWE, ist eine gemeinschaftlich entwickelte Liste von Schwächen: Bedingungen in Software, Firmware, Hardware oder einem Dienst, die unter passenden Umständen eine Sicherheitslücke ermöglichen. Das CVE Program beschreibt CWEs als die Grundursachen von CVE Records. Eine CVE benennt einen Fehler in einem Produkt, eine CWE die dahinterliegende Fehlerart. SQL-Injection ist beispielsweise die Schwäche CWE-89. Jedes Produkt, bei dem dieser Fehler festgestellt wird, erhält eine eigene CVE-ID.

Wie es in der Praxis aussieht

Shellshock, die Bash-Schwachstelle von 2014, zeigt alle drei Systeme nebeneinander. cve.org stellt seine Einträge im CVE Record Format dar, einem JSON-Format. Der Anfang dieses Eintrags sieht so aus (Felder gekürzt und umgeordnet):

```
{
  "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 reservierte als CNA die ID am 9. September 2014 und veröffentlichte den Eintrag fünfzehn Tage später. Laut Beschreibung verarbeitet Bash bis Version 4.3 Text, der im Wert einer Umgebungsvariablen auf eine Funktionsdefinition folgt. Ein entfernter Angreifer kann dadurch über eine präparierte Umgebung beliebigen Code ausführen. Der Eintrag hält auch fest, dass die erste Korrektur fehlerhaft war und der danach weiterhin offene Teil eine eigene ID erhielt: CVE-2014-7169. Teams, die einmal patchten und dann aufhörten, blieben angreifbar.

Danach enthält der Eintrag Container aus drei verschiedenen Quellen. Der CNA-Container enthält Debians Beschreibung und Referenzen. Der CVE Program Container ergänzt eigene Referenzen. Ein dritter Container stammt von einem Authorized Data Publisher, trägt den Titel CISA ADP Vulnrichment und ergänzt die Informationen, die die CVE-ID allein nicht enthält:


```
{
  "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"
  }
}
```


Der Vektor schlüsselt die Begründung für 9,8 auf: ein Angriff über das Netzwerk mit geringer Komplexität, ohne benötigte Berechtigungen und ohne Nutzerinteraktion, mit hoher Auswirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Derselbe Container ordnet den Fehler CWE-78 zu, der Schwächenklasse für die Einschleusung von Betriebssystembefehlen, und vermerkt, dass CISA ihn am 28. Januar 2022 in den KEV-Katalog aufnahm. Ein Eintrag enthält damit eine ID aus dem CVE Program, eine Bewertung nach einer von FIRST veröffentlichten CVSS-Version und eine Schwächenklasse aus CWE. Jede stammt aus einer anderen Quelle und beantwortet eine andere Frage.

Im Alltag sind CVE-IDs weniger Lesestoff als Schlüssel. Die Sicherheitsseite beschreibt die Routine: Die Bestandteile jedes Systems werden aufgelistet, und die Liste wird mit veröffentlichten Sicherheitshinweisen abgeglichen, statt den Bestandteilen zu vertrauen, weil sie bisher funktioniert haben. Über die CVE-ID lässt sich ein Befund dieser Prüfung zum Sicherheitshinweis zurückverfolgen und weiter zum Upgrade, das ihn behebt.

Wo es schiefgeht

Die Bewertung wird als Risiko gelesen. Wenn niemand Threat- oder Environmental-Werte liefert, setzt die CVSS-4.0-Spezifikation Standardwerte ein, die vom schlimmsten Fall ausgehen. Sie weist darauf hin, dass NVD und Produktverantwortliche normalerweise nur den Base-Wert veröffentlichen. Eine 9,8 für eine von außen unerreichbare Komponente ist für Sie keine 9,8. Kennzeichnen Sie Bewertungen gemäß der Spezifikation: CVSS-B für Base allein und CVSS-BTE, wenn Threat- und Environmental-Werte einbezogen wurden. Ergänzen Sie die Environmental-Werte für Ihre eigenen Systeme, bevor Sie die Arbeit priorisieren.

CVE, CVSS und CWE werden verwechselt. „Eine CVE von 9,8“ vermischt eine Kennung mit einer Bewertung, und „die SQL-Injection-CVE“ einen Fehler mit einer Fehlerklasse. Halten Sie die drei in Tickets und Berichten auseinander: die ID aus CVE, den Wert samt Version aus CVSS und die Grundursache aus CWE.

Eine Zahl wird ohne ihren Vektor genannt. FIRST verlangt von jedem, der CVSS-Daten veröffentlicht, auch den Vektor neben der Zahl zu veröffentlichen. So lassen sich die zugrunde liegenden Entscheidungen prüfen. Eine bloße Zahl kann weder überprüft noch zwischen CVSS-Versionen verglichen oder an die eigene Umgebung angepasst werden. Speichern Sie den vollständigen Vektor einschließlich des Präfixes `CVSS:3.1/` oder `CVSS:4.0/`, das die Version benennt.

Die Jahreszahl wird als Entdeckungsdatum gelesen. Das Jahr in der ID bezeichnet die Reservierung der ID oder die Veröffentlichung der Schwachstelle. Eine ID von 2014 kann in den 1990er-Jahren ausgelieferten Code beschreiben, und eine im Dezember entdeckte Schwachstelle kann eine Nummer des Folgejahres tragen. Verwenden Sie für Datumsangaben die Felder `dateReserved` und `datePublished` des Eintrags, nie die ID.

Es werden vier Ziffern vorausgesetzt. Die Folgenummer hat vier oder mehr Ziffern ohne Obergrenze. Ein Muster wie `CVE-\d{4}-\d{4}` schneidet längere IDs deshalb unbemerkt ab. Verwenden Sie stattdessen `^CVE-[0-9]{4}-[0-9]{4,}$` und behandeln Sie die ID als Zeichenfolge statt als Zahl, damit führende Nullen erhalten bleiben.

Ein Rejected-Eintrag wird als fehlend behandelt. Eine Rejected-ID bleibt absichtlich auf der Liste, um Nutzern ihre Ungültigkeit anzuzeigen. Werkzeuge, die sie ignorieren oder als offenen Befund zählen, führen in beiden Richtungen in

die Irre. Lesen Sie das Feld `state` und behandeln Sie `REJECTED` ausdrücklich.

Der Eintrag gilt als abgeschlossen. Der Shellshock-Eintrag wurde zuletzt im Oktober 2025 geändert, elf Jahre nach seiner Veröffentlichung. Sein KEV-Eintrag kam im Januar 2022 hinzu. Die CVSS-Spezifikation berücksichtigt mit der Threat-Gruppe, dass sich die Umstände einer Schwachstelle mit der Zeit ändern. Lesen Sie die Einträge hinter jedem Befund, den Sie akzeptiert statt behoben haben, regelmäßig erneut.

Die Arbeit endet nach der ersten Korrektur. Shellshock brauchte eine zweite ID, weil der erste Patch einen Teil des Fehlers offenließ. Lesen Sie Beschreibung und Referenzen jedes Eintrags auf nachfolgende IDs hin und schließen Sie einen Befund erst, wenn jede die Komponente betreffende ID erledigt ist.

Keine CVE gilt als keine Schwachstelle. CVE erfasst öffentlich bekannt gemachte Schwachstellen, denen eine CNA innerhalb ihres Zuständigkeitsbereichs eine ID zugewiesen hat. Ein Fehler im eigenen Code hat keine CVE, bis jemand ihn meldet und veröffentlicht. Der Abgleich von Abhängigkeiten mit der Liste deckt ab, was andere gefunden haben. Der eigene Code braucht eigene statische Analyse, Review und Tests.

Weiterführende Lektüre

- CVE Program: Überblick — Aufgabe, CVE Record und die Partner, die Einträge zuweisen und veröffentlichen.
- CVE Program: Verfahren — ID-Format, Mindestinhalt eines Eintrags und seine drei Zustände.
- CVE Program: verwandte Initiativen — die Beziehungen von NVD, CVSS, KEV-Katalog und CWE zu CVE und ihre Unterschiede.
- Common Vulnerability Scoring System v4.0: Spezifikation — die Metrikgruppen, Bewertungskennzeichnungen und qualitative Schweregradskala von FIRST.

- CVE Record Format — die JSON-Definition der Eintragsstruktur in der von CVE Services verwendeten Version.

- CVE Program: häufige Fragen (Archiv)

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist CVE?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

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

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/glossary/cve/