Engineer

CVE

den offentlige liste, der giver hver kendt sårbarhed ét id

Hvad det er

CVE, en forkortelse af Common Vulnerabilities and Exposures, er det offentlige katalog over offentligt kendte sårbarheder inden for it-sikkerhed, med én CVE-post for hver. CVE-programmet beskriver sin opgave som at identificere, definere og katalogisere de sårbarheder, så to personer eller to værktøjer kan henvise til en fejl og vide, at de taler om den samme. Ordet bruges om programmet, om listen og løst om en enkelt post, som når man siger, at et bibliotek har to åbne CVE'er.

Hver post har et CVE-id. Formatet er præfikset `CVE`, et firecifret årstal og et løbenummer på fire eller flere cifre, så `CVE-1999-0067`, `CVE-2019-12345` og `CVE-2021-7654321` er alle gyldige; programmet sætter ingen øvre grænse for, hvor mange cifre løbenummeret må have. Årstallet er det år, id'et blev reserveret, eller det år, sårbarheden blev offentliggjort. Programmet understreger selv, at årstallet ikke fortæller, hvornår sårbarheden blev opdaget.

Id'erne deles ikke ud fra ét centralt kontor. CVE Numbering Authorities, kaldet CNA'er, er leverandører, forskere, open source-projekter, it-beredskabsteams, operatører af onlinetjenester, udbydere af bug bounty-programmer og konsortier, som programmet har givet lov til at tildele id'er og udgive poster, hver inden for sit eget område. Hver eneste CVE-post er tilføjet af en CNA, der er hverken gebyr eller kontrakt forbundet med at blive en, og siden 2016 har programmet aktivt arbejdet på at få flere med.

En post gennemløber tre tilstande. Den starter som Reserved, når en CNA har taget et id, som de involverede bruger til at koordinere det tidlige arbejde med sårbarheden, inden den offentliggøres. Den bliver Published, når CNA'en har

udfyldt mindst id'et, en kort beskrivelse, de berørte produkter og versioner og en offentlig reference. Skal id'et ikke længere bruges, bliver det Rejected, og posten bliver stående på listen, så alle, der har id'et, kan se, at det er ugyldigt.

Idéen er fra 1999. To ingeniører fra MITRE, David E. Mann og Steven M. Christey, præsenterede konceptet i en hvidbog på en workshop på Purdue University i januar 1999, og listen blev offentlig i september samme år med 321 poster.

Brug begrebet i en beslutning

Brug »Hvad er CVE?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Konti, adgangskoder og rettigheder sat op, så folk har præcis den adgang, jobbet kræver, og fratrådte mister den samme dag.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har skrevet 1.000 RBAC-regler til Linux-servere — 1,000 adgangsregler skrevet for at lukke et sikkerhedshul

Har skrevet 1.000 RBAC-regler til Linux-servere Kontakt os →

Hvorfor det betyder noget

En sårbarhedsrapport er kun nyttig, hvis læseren kan afgøre, om den handler om det samme problem som en anden rapport. Det spørgsmål afgør et CVE-id: to sikkerhedsadvarsler, et fund fra en scanner og en sag i et sagssystem, der bærer det samme id, handler om den samme fejl. Mange store leverandører af styresystemer skriver CVE-id'er i deres sikkerhedsadvarsler, så alle har id'et fra det øjeblik, et problem bliver kendt, og sikkerhedsprodukter og -tjenester verden over bygger CVE-poster ind i det, de rapporterer.

Andre tjenester bygger på listen i stedet for ved siden af den. Den amerikanske National Vulnerability Database, som NIST lancerede i 2005, er et separat program, der bygger videre på CVE-posterne og føjer sine egne oplysninger til hver af dem. CISA's katalog over Known Exploited Vulnerabilities (KEV) samler fejl, som angribere er set udnytte, og hver post i det er identificeret ved og linker til en CVE-post.

Det vigtigste at vide om CVE er, hvad det ikke er. Det er ikke en score for alvorlighed: det er Common Vulnerability Scoring System, CVSS, en separat standard, som FIRST står for, en amerikansk nonprofitorganisation, hvis formål er at hjælpe it-sikkerhedsberedskaber i hele verden. CVSS version 4.0 vurderer en sårbarhed fra 0 til 10 ud fra fire grupper af målinger, Base, Threat, Environmental og Supplemental, og oversætter tallet til None, Low, Medium, High og Critical,

hvor Critical går fra 9,0 til 10,0. CVE Record Format lader en CNA lægge en CVSS-score ind i sin post, men scoren hører til CVSS og ikke til id'et: den samme fejl kan have forskellige scorer fra forskellige udgivere, eller ingen.

Det er heller ikke en kategori af svagheder. Common Weakness Enumeration, CWE, er en liste over svagheder, udviklet af fællesskabet: forhold i software, firmware, hardware eller en tjeneste, som under visse omstændigheder kan åbne for en sårbarhed. CVE-programmet beskriver CWE'er som grundårsagerne bag CVE-poster. En CVE navngiver én fejl i ét produkt; en CWE navngiver den slags fejl, der ligger bag. SQL-injection er for eksempel svagheden CWE-89, og hvert produkt, der viser sig at have begået netop den fejl, får sit eget CVE-id.

Sådan ser det ud i praksis

Shellshock, fejlen i Bash fra 2014, viser alle tre systemer side om side. cve.org viser sine poster i CVE Record Format, et JSON-format, og toppen af denne post ser sådan ud (felter udeladt og flyttet rundt):


```
{
  "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 reserverede som CNA id'et den 9. september 2014 og udgav posten femten dage senere. Beskrivelsen siger, at Bash til og med version 4.3 behandler tekst, der står efter en funktionsdefinition i værdien af en miljøvariabel, og at en angriber udefra derfor kan køre vilkårlig kode gennem et tilrettelagt miljø. Posten noterer også, at den første rettelse var forkert, og at den del, der stadig stod åben bagefter, fik sit eget id, CVE-2014-7169. Den, der kun opdaterede én gang og så stoppede, var stadig sårbar.

Posten rummer derefter containere fra tre forskellige kilder. CNA-containeren indeholder Debians beskrivelse og referencer. CVE Program Container tilføjer sine egne referencer. Den tredje kommer fra en Authorized Data Publisher, har titlen CISA ADP Vulnrichment og tilføjer det, som CVE-id'et alene ikke fortæller:

```
{
  "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"
  }
}
```

Vektorstrengen viser ræsonnementet bag 9,8: et angreb over netværket, med lav kompleksitet, uden krav om rettigheder og uden at en bruger skal gøre noget, med stor indvirkning på fortrolighed, integritet og tilgængelighed. Den samme container knytter fejlen til CWE-78, svaghedskategorien for injektion af kommandoer til styresystemet, og noterer, at CISA føjede den til KEV-kataloget den 28. januar 2022. En enkelt post rummer altså et id fra CVE-programmet, en score fra en CVSS-version, som FIRST udgiver, og en svaghedskategori fra CWE, hver fra sin egen kilde og hver som svar på sit eget spørgsmål.

I hverdagen betyder CVE-id'er mindre som læsestof end som nøgler. Vores sikkerhedsside beskriver rutinen: de dele, hvert system er bygget af, bliver skrevet ned, og listen holdes op mod offentliggjorte sikkerhedsadvarsler i stedet for at blive stolet på, fordi den virkede før. CVE-id'et er det, der gør, at et fund fra det tjek kan spores tilbage til advarslen og frem til den opdatering, der lukker hullet.

Hvor det går galt

At læse scoren som risikoen. Når ingen angiver værdier for Threat og Environmental, udfylder CVSS 4.0-specifikationen dem med standardværdier, der antager det værste, og den bemærker, at NVD og produktvedligeholdere som regel kun udgiver Base-scoren. En 9,8 på en komponent, der ikke kan nås udefra, er ikke en 9,8 for jer. Mærk scorerne, som specifikationen beder om, CVSS-B for kun Base og CVSS-BTE, når der er brugt værdier for Threat og Environmental, og tilføj Environmental-værdierne for jeres egne systemer, før I prioriterer arbejdet.

At blande CVE, CVSS og CWE sammen. »En CVE på 9,8« blander et id med en score, og »SQL-injection-CVE'en« blander en fejl med en kategori af fejl. Hold de tre adskilt i sager og rapporter: id'et fra CVE, scoren med sin version fra CVSS og grundårsagen fra CWE.

At angive et tal uden vektor. FIRST kræver, at alle, der udgiver CVSS-data, oplyser både scoren og vektorstrengen, så andre kan se, hvordan scoren er fremkommet. Et nøgent tal kan ikke efterprøves, sammenlignes på tværs af CVSS-versioner eller tilpasses jeres forhold. Gem hele vektoren, inklusive præfikset `CVSS:3.1/` eller `CVSS:4.0/`, der angiver versionen.

At læse årstallet som opdagelsesdatoen. Årstallet i id'et er det år, id'et blev reserveret, eller fejlen blev offentlig. Et id fra 2014 kan beskrive kode, der blev udgivet i 1990'erne, og en fejl, der bliver fundet i december, kan få det næste års nummer. Brug postens felter `dateReserved` og `datePublished` til datoer, aldrig id'et.

At gå ud fra fire cifre. Løbenummeret har fire eller flere cifre uden øvre grænse, så et mønster som `CVE-\d{4}-\d{4}` uden videre skærer længere id'er af. Match `^CVE-[0-9]{4}-[0-9]{4,}$` i stedet, og behandl id'et som en tekststreng og ikke som et tal, så foranstillede nuller bevares.

At behandle en Rejected-post som forsvundet. Et afvist id bliver med vilje stående på listen for at fortælle brugerne, at det er ugyldigt. Værktøjer, der overser det eller tæller det som et åbent fund, vildleder i hver sin retning. Læs feltet `state`, og håndter `REJECTED` udtrykkeligt.

At betragte posten som færdig. Shellshock-posten blev senest ændret i oktober 2025, elleve år efter at den blev udgivet, og dens KEV-oplysning kom til i januar 2022. CVSS-specifikationen beskriver sin Threat-gruppe som de egenskaber ved en sårbarhed, der ændrer sig over tid. Læs posterne bag de fund, I har accepteret i stedet for at rette, igen med faste mellemrum.

At stoppe ved den første rettelse. Shellshock fik et ekstra id, fordi den første rettelse lod en del af fejlen stå åben. Gennemgå hver posts beskrivelse og referencer for opfølgende id'er, og luk først et fund, når alle id'er, der nævner komponenten, er løst.

At tage fravær af en CVE som fravær af en sårbarhed. CVE dækker sårbarheder, der er offentliggjort og har fået et id af en CNA inden for dens område. En fejl i jeres egen kode har ingen CVE, før nogen rapporterer og offentliggør den. At scanne afhængigheder mod listen dækker det, andre har fundet; jeres egen kode kræver sin egen statiske analyse, gennemgang og test.

Læs mere

- CVE Program: Overview — programmets opgave, CVE-posten og de partnere, der tildeler og udgiver posterne.
- CVE Program: Process — id-formatet, det mindste indhold i en post og postens tre tilstande.
- CVE Program: Related Efforts — hvordan NVD, CVSS, KEV-kataloget og CWE hænger sammen med CVE, og hvor de adskiller sig.
- Common Vulnerability Scoring System v4.0: Specification Document — FIRST's grupper af målinger, betegnelserne for scorer og den kvalitative skala for alvorlighed.
- CVE Record Format — JSON-definitionen af, hvordan en post er opbygget, i den version, CVE Services bruger.
- CVE Program: FAQs (archive)

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er CVE?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

welcome@engineer.company +45 50 10 61 84 København, Danmark

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/cve/