WWW.PRO-SEC.DK

PROVISION ISR®
VÆRNER OM DIT PRIVATLIV

CVE - HVORFOR BETYDER DET NOGET FOR DIN SIKKERHED

Hold styr på sikkerhedshuller

OPDAGELSE

En forsker, etisk hacker eller et sikkerhedsværktøj opdager en ny sårbarhed i et produkt (HW, SW, FW).

RAPPORTERING

Fejlen bliver rapporteret til producenten eller en CVE Numbering Authority (CNA). Hvis producenten ikke reagerer, kan MITRE eller 3.parts CNA som ZDI (Zero Day Initiative) overtage sagen.

TILDELING AF ID

Hvis sårbarheden er reel, får den et unikt, officielt, globalt CVE-nr / reference for den pågældende fejl.

KOORDINERET OFFENTLIG-GØRELSE

60-90 Dage til at undersøge problemet, udvikle en rettelse og udarbejde vejledning til brugerne (streng fortroligt).

OFFENTLIG-GØRELSE

Når fejlen er rettet, offentliggøres CVE på cve.org. Info tilføjes NVD (National Vulnerability Database) og producent udsender sikkerhedsadvarsler.

SIKKERHEDS-REPONS

Når fejlen er rettet, offentliggøres CVE på cve.org. Info tilføjes NVD (National Vulnerability Database) og producent udsender sikkerhedsadvarsler.

Hvad er CVE?

CVE står for *Common Vulnerabilities and Exposures* – altså "almindelige sårbarheder og eksponeringer". Det er et globalt system, der bruges til at identificere og holde styr på sikkerhedshuller i software og hardware.

Hver sårbarhed får sit eget unikke CVE-ID, så producenter, sikkerhedseksperter og IT-folk kan tale samme sprog, når de skal finde og fikse problemer.

Tænk på det som en slags tilbagekaldelse af et produkt – bare for softwarefejl, som hackere kan udnytte.

Hvem står bag CVE?

CVE-programmet drives af MITRE Corporation, en amerikansk nonprofitorganisation, som arbejder under det amerikanske Department of Homeland Security og får finansiering fra CISA (Cybersecurity and Infrastructure Security Agency).

Formålet med programmet er at:

- gøre det ensartet, hvordan sårbarheder bliver rapporteret og registreret
- gøre det lettere for flere parter at samarbejde om at rette den samme fejl
- øge gennemsigtigheden og styrke cybersikkerheden globalt

De organisationer, der må udstede CVE-numre, kaldes CVE Numbering Authorities (CNAs). Det er bl.a. store spillere som Microsoft, Apple, Cisco, Intel, Google, Check Point og Amazon Web Services (AWS).

Provision-ISR og Check Point – et partnerskab om cybersikkerhed

Provision-ISR er dedikeret til at levere sikre og driftssikre overvågningssystemer. For at leve op til det løfte samarbejder vi med Check Point, en global frontløber inden for cybersikkerhed. Sådan hjælper samarbejdet både os og vores kunder:

- Hver ny Provision-ISR-model eller firmwareversion sendes til Check Point for en fuld Risk Assessment Report
- Rapporten gennemgår alle kendte sikkerhedshuller – både eksisterende CVE'er og potentielle "zero-day"-trusler
- Hvis der opdages sårbarheder, skal de rettes, før produktet frigives
- Intet Provision-ISR-produkt bliver lanceret uden at have bestået denne obligatoriske gennemgang

Ved at samarbejde med Check Point og følge internationale standarder som CVE, sikrer Provision-ISR, at både vores systemer og dine data er beskyttet fra dag ét.

Hvorfor CVE'er er vigtige?

Når en CVE bliver offentliggjort, betyder det:

- at producenten bliver advaret og kan lave en rettelse
- at brugere og IT-afdelinger bliver informeret om risikoen
- at virksomheder kan prioritere, hvilke opdateringer der haster mest

Uden CVE-systemet ville cybersikkerheds-verdenen være ren rodebutik – ingen fælles måde at spore fejl på, ingen koordination af løsninger og langt flere sårbare systemer.

Kort sagt:

Du behøver ikke være cybersikkerhedsekspert for at se værdien i CVE. Takket være vores proces slipper du for selv at holde øje med databaser og opdateringer.

Du kan stole på, at Provision-ISR:

- indbygger sikkerhed i hvert eneste produkt
- opdager og adresserer sårbarheder tidligt
- leverer videoovervågning, der lever op til branchens højeste standarder

Det her er cybersikkerhed bygget ind – ikke tilføjet bagefter.

ProSec A/S
Professional Security