Engineer

Har strammet systemd-sandboxen på hver unit

Har reduceret eksponeringen i systemd-sandkassen for hver unit, platformen installerer — en dead man's switch-tjeneste fra 9,6 UNSAFE til 1,5, en git-forge med adgang fra internettet fra 8,3 EXPOSED til 1,5 — og tilføjet et parsertjek ved konvergens efter at have fundet et fejlstavet direktiv, der ubemærket blev ignoreret i tre unit-skabeloner.

september 2026

hver unit lagt i sandkasse, og tastefejlen, der blev ignoreret

Situation. Tretten unit-filer blev installeret af dette repository og kører på produktionsværten med de privilegier, supervisoren giver som standard, og det er de fleste. En hærdningsscore gav dead man's switch-tjenesten 9,6 og kaldte den usikker; den internetvendte git-forge fik 8,3 og betegnelsen eksponeret. Begge tal var korrekte, og ingen af dem havde ført til noget, for en score uden en tilknyttet tærskel er et tal, folk lærer at springe over.

Opgave. Hver enhed skulle have en sandkasse, der står i forhold til det, den reelt gør, og sandkasserne skulle have et tjek, for en forkert sandkasse fejler på den måde, at enheden starter og derefter går i stykker et sted, parseren ikke kan se.

Handling. Privilegiebegrænsninger kom ind i alle unit-skabeloner — et privilegieloft låst fast på enhedens egne privilegier, et systemkaldsfilter, begrænsede adressefamilier og hukommelse, der er skrivbar eller eksekverbar, men aldrig begge dele. De målte resultater: dead man's switch gik fra 9,6 til 1,5, forgen fra 8,3 til 1,5 og de to sikkerhedskopienheder fra 9,6 til 2,3 og 2,5. Arbejdet med dem afdækkede noget, der var mere værd end scorerne. Ét direktiv havde været stavet forkert i tre unit-skabeloner, lige så længe de roller havde eksisteret — et navn, der ser plausibelt ud, men ikke findes, og som supervisoren reagerer på ved at logge, at den ikke genkender nøglen, og starte enheden alligevel. En søgning efter et direktiv beviser, at det blev skrevet; kun parseren beviser, at det fik virkning. Derfor kører en verifikationsrolle nu hver

enhed gennem supervisorens egen verifikator under kørslen, og den inkluderes af alle roller, der installerer en enhed. Det, den stadig ikke kan se, står klart i de samme dokumenter: alle direktiver, der kan ødelægge disse enheder, ødelægger dem under kørsel, ikke ved parsning, og en score kan ikke afgøre, om et script stadig når sin sidste linje.

Resultat. Hver enhed kører med de privilegier, den har brug for, og ikke dem, den ikke har brug for; tallene er målt, ikke påstået, og den fejltype, hvor en tastefejl bliver til en kontrol, der i al stilhed mangler, får nu en kørsel til at fejle. Målingens grænser er noteret ved siden af den, og det er den del, der forhindrer den næste læser i at stole for meget på et grønt scoreinterval.

Brug erfaringen i jeres projekt

Brug »Har strammet systemd-sandboxen på hver unit« som udgangspunkt for en lignende udfordring i jeres organisation. Ydelserne bag arbejdet kan også bruges i jeres projekt. Hele opsætningen skrevet ned som filer, så den kan genskabes præcist og aldrig kun findes i én persons hoved.

Se vores ydelser Kontakt os →

Se bag resultatet

Læs om situationen, beslutningerne og resultatet i eksemplet. Vi kan drøfte, hvad der passer til jeres vilkår, og hvad der kræver en anden tilgang. Har strammet systemd-sandboxen på hver unit — hver unit lagt i sandkasse, og tastefejlen, der blev ignoreret

Se vores ydelser Kontakt os →

Har dine tjenester mere adgang, end de har brug for?

Tal om jeres projekt med den ingeniør, der har ansvaret for leverancen. Vi aftaler omfang, prisgrundlag og overdragelse skriftligt, før arbejdet begynder.

Rolle i opgaven: Site Reliability-ingeniør. Det trækker på Infrastruktur, Containere (Docker/Kubernetes), Automatisering & CI/CD, Linux & servere, Sikkerhed og Test & QA. Og når I alligevel er her, er vi ret dygtige til Infrastructure as Code, Containerisering & orkestrering, Systemadministration og Sikkerhed & adgangsstyring.

Kontakt os Se vores ydelser

Ét stykke af **en længere fortegnelse** — og det hele ligger her på sitet.

Hver post er skrevet på samme måde: situationen, opgaven, hvad vi gjorde, og hvad der ændrede sig.

Se hele fortegnelsen

Definér den ønskede forbedring

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 →

Har dine tjenester mere adgang, end de har brug for?

Spørg til beslutningerne bag »Har strammet systemd-sandboxen på hver unit«. I taler med mennesker, der kan forklare arbejdet og vurdere jeres eget projekt.

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/portfolio/cut-systemd-sandbox-exposure-on-every-unit/