Engineer

Minskade systemd-exponeringen för varje enhet

Minskade exponeringen i systemd-sandlådan för varje enhet som plattformen installerar — en tjänst för dödmansgrepp från 9,6 UNSAFE till 1,5, en internetexponerad git-forge från 8,3 EXPOSED till 1,5 — och lade till en parserkontroll vid konvergering efter att ha hittat ett felstavat direktiv som tyst ignorerades i tre enhetsmallar.

september 2026

varje enhet i sandlåda, och stavfelet som ignorerades

Situation. Tretton enhetsfiler installerades av det här repot och kördes på produktionsvärden med de privilegier som tjänstehanteraren ger som standard, och det är de flesta. En härdningspoäng gav dödmansgreppets tjänst 9,6 och omdömet osäker; den internetvända git-forgen fick 8,3 och omdömet exponerad. Båda siffrorna stämde och ingen av dem hade lett till något, eftersom en poäng utan ett tröskelvärde kopplat till sig är en siffra som folk lär sig att hoppa över.

Uppgift. Varje enhet behövde en sandlåda i proportion till vad den faktiskt gör, och sandlådorna behövde en kontroll, eftersom en felaktig sandlåda fallerar på så sätt att enheten startar och sedan går sönder någonstans där parsern inte kan se det.

Handling. Privilegiebegränsningar fördes in i varje enhetsmall — ett privilegietak låst vid enhetens egen nivå, ett filter för systemanrop, begränsade adressfamiljer och minne som är skrivbart eller körbart men aldrig båda. De uppmätta resultaten: dödmansgreppet gick från 9,6 till 1,5, git-forgen från 8,3 till 1,5 och båda enheterna för säkerhetskopiering från 9,6 till 2,3 respektive 2,5. När begränsningarna skrevs dök något upp som var bättre än poängen. Ett direktiv hade varit felstavat i tre enhetsmallar så länge de rollerna hade funnits — ett namn som ser trovärdigt ut men inte finns, och som tjänstehanteraren besvarar genom att logga att den inte känner igen nyckeln och sedan starta enheten ändå. Att greppa efter ett direktiv bevisar att det skrevs;

bara parsern bevisar att det fick effekt. Därför kör en verifieringsroll nu varje enhet genom tjänstehanterarens egen verifierare under konvergenskörningen, och den inkluderas av varje roll som installerar en enhet. Vad den fortfarande inte kan se står klart utskrivet i samma dokument: varje direktiv som kan få de här enheterna att gå sönder gör det vid körning, inte vid parsning, och en poäng kan inte avgöra om ett skript fortfarande når sin sista rad.

Resultat. Varje enhet körs med de privilegier den behöver och utan dem den inte behöver, siffrorna är uppmätta snarare än påstådda, och den typ av defekt där ett stavfel blir en åtgärd som i tysthet saknas får nu en körning att misslyckas. Mätningens begränsningar står antecknade bredvid den, och det är den delen som hindrar nästa läsare från att lita för mycket på ett grönt intervall.

Använd erfarenheten i ert projekt

Använd ”Minskade systemd-exponeringen för varje enhet” som utgångspunkt för en liknande utmaning i er organisation. Tjänsterna bakom arbetet finns tillgängliga för ert projekt. Hela uppsättningen nedskriven som filer, så att den kan återskapas exakt och aldrig bara finns i en enda persons huvud.

Se våra tjänster Hör av er →

Se bakom resultatet

Läs om situationen, besluten och resultatet i exemplet. Vi kan diskutera vad som passar era förutsättningar och vad som kräver ett annat angreppssätt. Minskade systemd-exponeringen för varje enhet — varje enhet i sandlåda, och stavfelet som ignorerades

Se våra tjänster Hör av er →

Har dina tjänster mer åtkomst än de behöver?

Prata om ert projekt med ingenjören som ansvarar för leveransen. Vi avtalar omfattning, hur priset beräknas och överlämning skriftligt innan arbetet börjar.

Roll i uppdraget: Site Reliability Engineer. Det bygger på Infrastruktur, Containrar (Docker/Kubernetes), Automatisering och CI/CD, Linux och servrar, Säkerhet och Test och kvalitetssäkring. Och nu när ni är här: vi är ganska bra på Infrastruktur som kod, Containerisering och orkestrering, Systemadministration och Säkerhet och behörighetshantering.

Hör av er Se våra tjänster

En del av **en längre historik** — och den finns i sin helhet här.

Varje post är skriven på samma sätt: situationen, uppgiften, vad vi gjorde och vad som förändrades.

Se hela historiken

Definiera förbättringen ni behöver

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Har dina tjänster mer åtkomst än de behöver?

Fråga om besluten bakom ”Minskade systemd-exponeringen för varje enhet”. Ni talar med personer som kan förklara arbetet och bedöma ert eget projekt.

Se våra tjänster

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

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/portfolio/cut-systemd-sandbox-exposure-on-every-unit/