Engineer

Alle systemd-Units stärker isoliert

Die Angriffsfläche der systemd-Sandboxen für jede von der Plattform installierte Unit verringert — einen Totmannschaltungsdienst von 9,6 UNSAFE auf 1,5, eine internetseitig erreichbare Git-Forge von 8,3 EXPOSED auf 1,5 — und eine Parserprüfung beim Konvergenzlauf ergänzt, nachdem eine falsch geschriebene Direktive in drei Unit-Vorlagen stillschweigend ignoriert worden war.

September 2026

jede Unit isoliert und der ignorierte Tippfehler gefunden

Situation. Dreizehn von diesem Repository installierte Unit-Dateien liefen auf dem Produktivhost mit den standardmäßig umfangreichen Rechten des Prozessmanagers. Eine Härtungsbewertung gab dem Totmannschaltungsdienst 9,6 und die Einstufung unsafe; die internetseitig erreichbare Git-Forge erhielt 8,3 und exposed. Beide Werte waren richtig und hatten nichts ausgelöst. Eine Zahl ohne Schwelle wird leicht überlesen.

Aufgabe. Jede Unit brauchte eine zu ihrer tatsächlichen Aufgabe passende Sandbox. Auch die Sandboxen brauchten Prüfungen, denn eine falsche Sandbox lässt eine Unit oft starten und erst später außerhalb der Parserreichweite scheitern.

Massnahmen. Jede Unit-Vorlage erhielt Beschränkungen: eine feste Obergrenze auf die eigenen Privilegien, Systemaufruffilter, begrenzte Adressfamilien und Speicher, der schreibbar oder ausführbar, aber nie beides sein darf. Die gemessenen Ergebnisse: Totmannschaltung von 9,6 auf 1,5, Forge von 8,3 auf 1,5 und die beiden Sicherungsunits von 9,6 auf 2,3 beziehungsweise 2,5. Beim Schreiben zeigte sich etwas Wertvolleres als die Bewertungen. Eine Direktive war seit Entstehung der Rollen in drei Unit-Vorlagen falsch geschrieben: ein plausibel klingender, aber nicht existierender Name. Der Prozessmanager protokolliert den unbekannten Schlüssel und startet die Unit trotzdem. Textsuche beweist nur das Schreiben; erst der Parser bestätigt die Wirksamkeit. Eine Verifikationsrolle lässt deshalb während der Konvergenz jede Unit durch den

eigenen Verifizierer des Prozessmanagers laufen. Jede Unit-installierende Rolle bindet sie ein. Die verbleibende Grenze steht in denselben Dokumenten: Alle diese Units gefährdenden Direktiven wirken zur Laufzeit, nicht beim Parsen. Eine Bewertung zeigt nicht, ob ein Skript seine letzte Zeile noch erreicht.

Ergebnis. Jede Unit läuft mit den benötigten und ohne überflüssige Rechte. Die Werte sind gemessen statt behauptet. Fehler, bei denen ein Tippfehler stillschweigend eine Kontrolle entfernt, lassen den Lauf nun scheitern. Die Messgrenzen stehen direkt daneben und verhindern, dass die nächste lesende Person einer grünen Einstufung zu viel vertraut.

Diese Erfahrung für Ihr Projekt nutzen

Nutzen Sie „Alle systemd-Units stärker isoliert“ als Ausgangspunkt für eine ähnliche Herausforderung in Ihrer Organisation. Die Leistungen hinter dieser Arbeit stehen auch für Ihr Projekt zur Verfügung. Die gesamte Einrichtung wird in Dateien festgehalten, damit sie sich exakt wiederherstellen lässt und nicht nur im Kopf einer einzelnen Person existiert.

Unsere Leistungen entdecken Kontakt aufnehmen →

Hinter das Ergebnis schauen

Lesen Sie die Situation, die Entscheidungen und das Ergebnis dieses Beispiels. Wir können besprechen, welche Teile sich auf Ihre Rahmenbedingungen übertragen lassen und welche einen anderen Ansatz erfordern. Alle systemd-Units stärker isoliert — jede Unit isoliert und der ignorierte Tippfehler gefunden

Unsere Leistungen entdecken Kontakt aufnehmen →

Haben Ihre Dienste mehr Zugriff als nötig?

Besprechen Sie Ihr Projekt mit der Ingenieurin, die für die Umsetzung verantwortlich ist. Wir vereinbaren Umfang, Preisgrundlage und Übergabe schriftlich, bevor die Arbeit beginnt.

Rollenkontext: Site Reliability Engineer. Die Arbeit baut auf Infrastruktur, Container (Docker/Kubernetes), Automatisierung und CI/CD, Linux und Server, Sicherheit und Tests und Qualitätssicherung. Und wenn Sie schon hier sind: Wir sind auch ziemlich gut in Infrastructure as Code, Containerisierung und Orchestrierung, Systemadministration und Sicherheits- und Zugriffsverwaltung.

Kontakt aufnehmen Unsere Leistungen entdecken

Ein Teil einer **längeren Arbeitsbilanz** — vollständig auf dieser Website zu finden.

Jeder Eintrag folgt demselben Aufbau: die Situation, die Aufgabe, unser Vorgehen und die Veränderungen.

Alle Arbeiten ansehen

Die benötigte Verbesserung definieren

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 →

Haben Ihre Dienste mehr Zugriff als nötig?

Fragen Sie nach den Entscheidungen hinter „Alle systemd-Units stärker isoliert“. Sie sprechen mit den Menschen, die die Arbeit erklären und Ihr eigenes Projekt einschätzen können.

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