AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësitë Kritike në Spring Boot

Data: 27/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Në Spring Boot, një strukturë Java i përdorur gjerësisht, janë zbuluar shumë dobësi me ndikim të lartë.

Informacione Teknike

Në Spring Boot, një strukturë Java e përdorur gjerësisht që mbështet miliona aplikacione ndërmarrjesh, janë zbuluar shumë dobësi me ndikim të lartë. Gabimi më kritik (CVSS 9.1) mund të anashkalojë plotësisht kontrollet e sigurisë së aplikacioneve sipas konfigurimeve specifike, duke i ekspozuar të gjitha pikat fundore ndaj aksesit të paautorizuar.

Detajet e dobësisë:
1. Anashkalimi i Autentifikimit nëpërmjet Keqkonfigurimit të Sigurisë Parazgjedhur
• ID e CVE: CVE-2026-40976
• Ashpërsia: Kritike (CVSS 9.1)
• Komponenti: Konfigurimi i Sigurisë së Uebit Parazgjedhur (nëpërmjet Spring Security)

Problemi Kryesor:
• Një gabim në zinxhirin e filtrit të sigurisë parazgjedhur mund të rezultojë në anashkalim të plotë të sigurisë, duke i lënë të gjitha pikat fundore të pambrojtura.

Kushtet për Shfrytëzim:
• Aplikacioni është i bazuar në servlet.
• Mbështetet vetëm në konfigurimin e sigurisë parazgjedhur (pa rregulla sigurie të personalizuara).
• Përfshin spring-boot-actuator-autoconfigure.
• Nuk përfshin varësinë spring-boot-health.
2. Sulmi i Kohës në DevTools që drejton në zbulimin e informacionit
• ID e CVE: CVE-2026-40972
• Ashpërsia: E Lartë (CVSS 7.5)
• Komponenti: Spring Boot DevTools
Problemi Kryesor:
• Një dobësi e kanalit anësor të kohës u lejon sulmuesve të nxjerrin te dhëna duke matur kohët e reagimit.
Vektori i Sulmit:
• Sulmuesi duhet të jetë në të njëjtin rrjet.
• Shfrytëzon krahasimin jo-konstant të sekreteve.

3. Trajtimi i pasigurt i Drejtorisë së Përkohshme
• ID e CVE: CVE-2026-40973
• Ashpërsia: E Lartë (CVSS 7.0)

• Komponenti: Trajtimi i direktorise ApplicationTemp
Problemi Kryesor:
• Përdorim i direktorise së përkohshme i parashikueshëm ose i kontrollueshëm.
Vektori i Sulmit:
• Kërkon qasje lokale në sistemin pritës.
• Ekzekuton kod arbitrar duke përdorur zinxhirë të pajisjeve të krijuara.
• Përshkallëzim i privilegjit brenda kontekstit të aplikacionit.

Versionet e Prekura dhe Disponueshmëria e Rregullimeve
• 4.0.x → Rregulluar në 4.0.6 (OSS)
• 3.5.x → Rregulluar në 3.5.14 (OSS)
• 3.4.x → Rregulluar në 3.4.16 (Vetëm për Ndërmarrje)
• 3.3.x → Rregulluar në 3.3.19 (Vetëm për Ndërmarrje)
• 2.7.x → Rregulluar në 2.7.33 (Vetëm për Ndërmarrje)

Rekomandime

AKSK rekomandon te përmirësoni Spring Boot në versionin e përditësuar sa më shpejt të jetë e mundur.