THREAT INTELLIGENCE BRIEFING

CVE-2026-59415

Massenlöschung von KI-Wissensdaten in Spring AI (Typesense-Anbindung).

Spring AI ist das Java-Framework, mit dem Unternehmen KI-Funktionen wie Chatbots und Wissenssuche (RAG) in ihre Spring-Anwendungen einbauen. Die Anbindung an die Vektordatenbank Typesense setzt Dokument-IDs beim Löschen ungeprüft in einen Filterausdruck ein. Wer eine solche ID beeinflussen kann, löscht fremde Dokumente oder den gesamten Wissensbestand. Betroffen sind Anwendungen, die von außen kommende IDs an die Löschfunktion weitergeben. Die Fixversion 2.0.3 ist verfügbar; eine Ausnutzung ist bisher nicht bekannt.

> **Geschäftsrisiko:** Verlust des Wissensbestands hinter KI-Assistenten und Suchfunktionen, Ausfall der darauf aufbauenden Anwendungen und Aufwand für die Wiederherstellung; je nach Daten ein möglicherweise meldepflichtiger Vorfall nach NIS-2 / DSGVO.

10,0 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H` – aus dem Netz, ohne Anmeldung, ohne Mitwirkung eines Nutzers. Basiswert laut CNA (VMware), vom NVD übernommen. Die Spring-Advisory-Seite selbst stuft die Lücke als „hoch“ ein (verlinkter Vektor 8,1, ohne Wirkung auf Vertraulichkeit).

AUSNUTZUNG
Nicht bekannt (Stand 24.11.2026)

BETROFFEN
Spring AI 2.0.0–2.0.2, 1.1.0–1.1.9, 1.0.0–1.0.10
(nur mit TypesenseVectorStore)

HANDLUNGSBEDARF
Dringend – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

10,0 · KRITISCH
CVSS-Schweregrad (CNA/NVD)

Ohne Anmeldung
Filter-Injection über Dokument-IDs · CWE-917

Nicht bekannt
Ausnutzung · nicht in CISA KEV · kein PoC öffentlich

2.0.3
Fixversion (OSS) · ältere Zweige nur Enterprise

Die Ursache: `TypesenseVectorStore.doDelete()` baut den Filter `id: [id1,id2,...]` durch **einfaches Aneinanderhängen der IDs**, ohne Anführungszeichen und ohne Escaping (**CWE-917**). Ein Komma, eine Klammer `]` oder Operatoren wie `||` in einer ID verändern den Filter: Gelöscht werden fremde oder alle Dokumente der Collection.

ANGRIFFSKETTE

01 **Einstieg** – Anwendung reicht eine von außen kommende Dokument-ID an delete() weiter

02 **Präparierte ID** – Komma,] oder || && im Wert

03 **Filter gekapert** – der Ausdruck trifft fremde oder alle Dokumente

04 **Massenlöschung** – Wissensbestand der KI-Anwendung ist weg

Betroffenheit & Fixversionen

Spring-AI-Version	Verwundbar bis	Fixversion (Ziel)
2.0.x (OSS)	`2.0.0 – 2.0.2`	`2.0.3`
2.0.x (Enterprise)	`2.0.0 – 2.0.2`	`2.0.2.1`
1.1.x (Enterprise)	`1.1.0 – 1.1.9`	`1.1.10`
1.0.x (Enterprise)	`1.0.0 – 1.0.10`	`1.0.11`

Laut Spring-Advisory (19.11.2026). Betroffen nur mit `TypesenseVectorStore` und externen IDs an `delete()`. **Fixe für 1.0.x/1.1.x nur mit Enterprise-Support – sonst auf 2.0.3 wechseln.**

Regulatorischer Hinweis: Ein bestätigter unbefugter Eingriff in Datenbestände kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

04.07.2026
CVE-Nummer reserviert

19.11.2026
Spring-Advisory · Fix 2.0.3

24.11.2026
CVE-Record und NVD veröffentlicht

Stand heute
Nicht in CISA KEV · kein PoC

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – erst Betroffenheit, dann Patch, dann Kontrolle.

SOFORT	KURZFRISTIG	PARALLEL
Betroffenheit klären	Update auf 2.0.3	IDs prüfen, Backups sichern

01 Betroffenheit feststellen

In allen Java-Anwendungen nach der Abhängigkeit `spring-ai-typesense-store` bzw. `TypesenseVectorStore` suchen (SBOM, `mvn dependency:tree`). Klären, ob Dokument-IDs aus Anfragen, Formularen oder Schnittstellen an die Löschfunktion gehen.

02 Patchen

Auf `2.0.3` aktualisieren. Mit Enterprise-Support: `2.0.2.1`, `1.1.10` oder `1.0.11`. Ohne Support auf 1.x ist der Wechsel auf 2.0.3 der Weg zum Fix.

03 Übergangsweise IDs prüfen

Jede ID vor `delete()` gegen eine Positivliste prüfen: Buchstaben, Ziffern, `- _ . : / @`. Alles andere ablehnen. IDs aus `UUID.randomUUID()` oder base64url gelten laut Spring als sicher.

04 Bestand kontrollieren

Typesense-Collections auf unerklärliche Dokumentverluste prüfen und Backups bzw. Snapshots sichern, damit sich der Wissensbestand wiederherstellen lässt.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – Spring nennt keine, Ausnutzung nicht bekannt

AUSWERTUNGSQUELLEN

Anwendungs-Logs der Löschaufrufe
Typesense-API-Logs

AUFFÄLLIGE MUSTER

Dokument-IDs mit `,` `]` `||` `&&`
plötzlicher Rückgang der Dokumentzahl

Zur Einordnung: Es liegen keine CVE-spezifischen Indikatoren vor. Die genannten Muster sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen.

Wichtig: KI-Anwendungen entstehen oft in Fachbereichen und Projekten außerhalb des regulären Patchmanagements. Ihre Bibliotheken gehören ins Schwachstellenmanagement wie jede andere Software.

Bildmotive: KI-generierte Symbolbilder

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

Worauf wir bei dieser Schwachstelle achten: Massenhafte Löschaufrufe gegen die Typesense-API. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden Spring-AI-Anwendungen mit Typesense-Anbindung über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre Spring AI-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Prüfung auf Angriffsspuren, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Update aller Spring-AI-Anwendungen mit Typesense auf 2.0.3 anordnen.
- KI-Projekte ins reguläre Schwachstellenmanagement aufnehmen.
- Wiederherstellbarkeit der KI-Wissensbestände prüfen lassen.

Ihr Part · unser Part. **Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.**

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2026-59415 und dem Spring AI-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Spring-Advisory CVE-2026-59415 (19.11.2026, Fixversionen, Einstufung „hoch“) · CVE.org / NVD (24.11.2026, CVSS 3.1 10,0 laut CNA VMware) · CISA KEV (Stand 24.11.2026: nicht gelistet). Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.