DEFION

SECURITY ADVISORY
18 NOVEMBER 2026

Kritieke kwetsbaarheid in Java (Java4Shell)

Via een kwetsbaarheid in OpenJDK is een Java-server op afstand over te nemen, vaak zonder inloggegevens. De patch is er sinds 17 november.

ERNST	KENMERK	STATUS
Kritiek (CVSS 4.0: 9,2)	CVE-2026-114938	Patch beschikbaar Publieke proof of concept

01 · KERNBOODSCHAP

In Java (OpenJDK) zit een kritieke kwetsbaarheid waarmee een aanvaller op afstand een server kan overnemen, vaak zonder inloggegevens. De patch is er sinds 17 november.

ONS ADVIES IN VIER PUNTEN

Patch internetgerichte Java-diensten binnen 72 uur. Zet tot die tijd een opstartvlag.

01 Bepaal wat eerst gaat
Internetgerichte Java-diensten die Base64 uit gebruikersinvoer decoderen, gaan eerst.

02 Vandaag niet patchen: opstartvlag
Start de JVM met -XX:-UseBASE64Intrinsics. Dat vraagt een herstart.

03 Patch binnen 72 uur
Eerst blootgestelde systemen, daarna interne.

04 Spreek uw leveranciers aan
Vraag welke Java-versie zij meeleveren en wanneer hun update verschijnt.

Weet u niet welke Java-versie een systeem draait, behandel het dan als kwetsbaar.

02 · WAT SPEELT ER

Eén Base64-reeks is genoeg

- Het gaat om **CVE-2026-114938**, bijgenaamd “Java4Shell”. Ernst: kritiek (CVSS 4.0: 9,2). Oracle hanteert onder CVSS 3.1 een 8,1.
- Eén speciaal opgebouwde Base64-reeks is genoeg om code op de server uit te voeren. Base64 zit in authenticatieheaders, sessietokens, SAML-berichten en API's.
- Kwetsbaar zijn OpenJDK vanaf 17.0.6 en alle afgeleide distributies, waaronder Oracle Java SE, Temurin, Corretto, Azul Zulu en Red Hat OpenJDK. Ook Oracle Java SE 8 Enterprise Performance Pack is kwetsbaar.
- Alleen op x86-64-processors met AVX-512 VBMI: Intel Xeon vanaf Ice Lake en AMD vanaf Zen 4. ARM64 is niet kwetsbaar.
- Aangetoond zonder authenticatie in Keycloak, Jira, Confluence, Artifactory, Jenkins en PingFederate. Met authenticatie in Kafka, Solr, Elasticsearch, Gerrit en Spinnaker.
- Er is een proof of concept openbaar. Actief misbruik is nog niet bevestigd.

03 · WAAR ZIT JAVA

Op meer plekken dan u denkt

Neem ook de Java-runtimes mee die leveranciers in hun producten meeleveren.

Eigen applicaties

Applicaties op Spring Boot, Apache Struts en andere Java-frameworks.

Identiteit en samenwerking

Keycloak, PingFederate, Jira en Confluence.

Ontwikkelstraat en data

Jenkins, Artifactory, Gerrit, Spinnaker, Kafka, Solr en Elasticsearch.

Systemen van derden

Producten en appliances met een eigen Java-runtime, en diensten die een leverancier voor u beheert.

> Kijk ook intern. Een Java-programma dat een TLS-verbinding opent naar een server van een aanvaller, is op dezelfde manier kwetsbaar.

Wat u nu doet

Voer stap 1 tot en met 4 vandaag uit. Stap 5 en 6 volgen binnen 72 uur.

Vandaag

Inventariseren en afschermen

01 Inventariseer waar Java draait

Breng elke JDK en JRE in kaart, ook in producten en appliances van derden.

- Begin bij internetgerichte diensten die Base64 uit gebruikersinvoer decoderen.
- Weet u de versie niet, behandel het systeem dan als kwetsbaar.

02 Controleer de processor

Op Linux is de host kwetsbaar als dit commando alle vier de vlaggen teruggeeft:

```
grep -m1 '^flags' /proc/cpuinfo | tr ' ' '\n' | grep -E '^(avx512f|avx512bw|avx512vbmi|bmi2)$'
```

03 Niet direct patchen: zet een opstartvlag

Start de JVM met `-XX:-UseBASE64Intrinsics`. Het alternatief, alleen op x86-64, is `-XX:UseAVX=2`. Beide vragen een herstart van de dienst.

> Dit is een tijdelijke maatregel. De vlaggen beperken de blootstelling, maar vervangen de patch niet.

04 Benader derde partijen direct

Vraag elke leverancier en beheerpartij welke Java-versie zij meeleveren en wanneer hun update verschijnt.

Binnen 72 uur

Patchen en controleren

05 Patch naar de herstelde versie

Installeer de herstelde versie van uw distributeur. Eerst blootgestelde diensten, daarna interne systemen.

PRODUCT	KWETSBARE VERSIE	HERSTELDE VERSIE
Oracle Java SE 8 Enterprise Performance Pack	8u511b33-perf	8u513-perf
Oracle Java SE 17	17.0.21.0.3	17.0.21.1
Oracle Java SE 21	21.0.13.0.3	21.0.13.1
Oracle Java SE 25	25.0.5.0.3	25.0.5.1
Oracle Java SE 27	27.0.1.0.3	27.0.1.1
Amazon Corretto 17	niet vermeld	17.0.21.1.2

Andere distributeurs volgen hun eigen planning. Controleer hun advisory.

06 Controleer op misbruik

Doe dit voordat u een systeem schoon verklaart.

- Crashes van de JVM en nieuwe `hs_err_pid*.log`-bestanden.
- Herhaalde herstarts van dezelfde Java-dienst in korte tijd.
- Ongewoon lange Base64-invoer of afwijkende padding in headers, cookies en SAML-berichten.
- Onverwachte childprocessen van de JVM en nieuwe uitgaande verbindingen.
- Vindt u sporen, isoleer het systeem dan en schakel incident response in.

Doorlopend

Verhoogde waakzaamheid

- Laat uw SOC of beheerpartij deze signalen volgen tot alles is gepatcht.
- Blijf de komende dagen alert. De onderzoekers hebben exploitketens per product aangekondigd.

05 · VEELGESTELDE VRAGEN

Als u doorvraagt

Onze servers zijn ARM. Zijn wij kwetsbaar?

Nee. Werk toch bij: workloads kunnen altijd naar andere hardware verhuizen.

Helpt een webapplicatiefirewall?

Maar gedeeltelijk. De invoer lijkt op gewone Base64 en is lastig te filteren zonder legitiem verkeer te breken.

Wij gebruiken Java 8 of 11. Zijn wij veilig?

Standaardbuilds vallen buiten het gepubliceerde bereik. De uitzondering is Oracle Java SE 8 Enterprise Performance Pack. Vraag uw distributeur om bevestiging.

Wat kan DEFION doen?

Wij brengen in kaart waar Java draait, zoeken naar sporen van misbruik, helpen bij het patchen en leveren incident response.

06 · VOOR UW SECURITYTEAM

De techniek in het kort

Out-of-bounds heap write in de Base64-intrinsic van HotSpot voor x86-64. Bij invoer met afwijkende padding wordt het schrijfmasker (`bzhiq`) verkeerd berekend en schrijft `evmovdqub` 64 bytes, tot 62 bytes voorbij het einde van de buffer. Trigger: `'A' * 64 + '='`, op OpenJDK 17 `'A' * 128 + '='`.

Bronnen: Calif, calif.io/java4shell · OpenJDK Vulnerability Advisory 2026-11-17 · Oracle Security Alerts · Tenable · Cisco Talos

CONTACT

+31 88 733 13 37

Vragen of hulp nodig? Neem contact op met uw directe contactpersoon bij DEFION of bel ons algemene nummer.

DEFION