Network Vulnerability Scanner Report

✔ 172.17.0.3

Summary

Overall risk level:

High

Risk ratings:

Critical:	0
High:	1
Medium:	0
Low:	0
Info:	2

Scan information:

Start time:	Nov 18, 2026 / 16:55:19 UTC+02
Finish time:	Nov 18, 2026 / 16:55:47 UTC+02
Scan duration:	28 sec
Tests performed:	6
VPN Profile:	mac-vpn
Scan status:	Finished

Findings

Java4Shell - OpenJDK Base64 Decoder Heap Overflow (CVE-2026-114938)

CONFIRMED

port 9200/tcp

We managed to detect this vulnerability using the following Request / Response chain.
We extracted the following information from the target: **Java 22.0.1**
Endpoint: **http://172.17.0.3:9200/_nodes/_local/jvm**

Details

Vulnerability description:

The x86-64 AVX-512 Base64 decoder intrinsic in the OpenJDK HotSpot JVM, used by java.util.Base64, writes past the end of the destination array when it decodes a short final block with padding. OpenJDK 17.0.6 and later is affected prior to 17.0.21.1, 21.0.13.1, 25.0.5.1 and 27.0.1.1, and the non-LTS lines 18 to 20, 22 to 24 and 26 receive no fix. Only JVMs running on CPUs with AVX-512 VBMI (Intel Ice Lake and newer Xeon, AMD Zen 4 and newer) reach the vulnerable code. Any application that Base64-decodes attacker-controlled input, for example in authentication headers, tokens or file uploads, can be exploited. The template is a passive version check and sends no exploit trigger. It reads the Java runtime version from endpoints that disclose it, namely the Apache Solr system info API, the Elasticsearch or OpenSearch nodes API, the Spring Boot Actuator env and info endpoints, the Quarkus info endpoint, the Jolokia and Hadoop JMX Runtime MBean, and the X-Powered-By header, and reports affected versions.

Risk description:

An unauthenticated attacker who can get the application to Base64-decode a crafted value can corrupt the JVM heap and potentially run code with the privileges of the Java process. Pre-authentication exploitation has been demonstrated against default installations of Keycloak, Jira, Confluence, Jenkins, JFrog Artifactory and PingFederate. A match is based only on the disclosed Java version. It does not confirm that the host CPU supports AVX-512 VBMI, that the JVM runs without the -XX:-UseBASE64Intrinsics or -XX:UseAVX=2 mitigation, or that a vendor build with the same version string has not been patched. Builds released before and after the November 2026 fix can share a version string, so a match should be confirmed on the host. The endpoints used for detection also disclose runtime details and are an exposure in their own right.

Recommendation:

Upgrade the Java runtime to a build that contains the November 2026 fix, for example Oracle JDK 17.0.21.1, 21.0.13.1, 25.0.5.1, 27.0.1.1 or later, or Amazon Corretto 17.0.21.1.2, 21.0.13.1.2, 25.0.5.1.2, 27.0.1.1.4 or later, and restart every JVM and rebuild container images that bundle a runtime. Move applications on Java 18 to 20, 22 to 24 or 26 to a supported line. For other distributions, follow the vendor advisory. Until you can patch, start the JVM with -XX:-UseBASE64Intrinsics, or with -XX:UseAVX=2 on x86-64 hosts only, and confirm the active flags with jcmd <pid> VM.flags -all. Restrict access to Solr, Elasticsearch, Actuator, Quarkus, Jolokia and JMX management endpoints.

References:

https://calif.io/java4shell/
https://openjdk.org/groups/vulnerability/advisories/2026-11-17
https://www.oracle.com/security-alerts/cspunov2026.html
https://www.openwall.com/lists/oss-security/2026/11/17/31
https://horizon3.ai/attack-research/vulnerabilities/cve-2026-114938/
https://nvd.nist.gov/vuln/detail/CVE-2026-114938
https://www.cve.org/CVERecord?id=CVE-2026-114938

Classification:

CISA KEV: False
CVE : CVE-2026-114938
CVSS V3 : 8.1

Open ports discovery

CONFIRMED

Port	State	Service	Product	Product Version
9200	open	wap-wsp	-	-

Details

Risk description:
This is the list of ports that have been found on the target host. Having unnecessary open ports may expose the target to more risks because those network services and applications may contain vulnerabilities.

Recommendation:
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

OS Detection

UNCONFIRMED

Operating System	Accuracy
Linux 2.6.32	95%

Details

Vulnerability description:
OS Detection

Scan coverage information

List of tests performed (6)

Port 9200

- ✔ Checked for "Java4Shell - OpenJDK Base64 Decoder Heap Overflow (CVE-2026-114938)"
- ✔ Scanned for version-based vulnerabilities

Generic tests

- ✔ Performed OS detection
- ✔ Performed port discovery
- ✔ Performed version-based engine detections
- ✔ Performed Nuclei engine detections

Scan parameters

Target:	172.17.0.3
Preset:	Custom
Scanning engines:	Version_based, Nuclei
Check alive:	True
Extensive modules:	False
Protocol type:	TCP
Ports to scan:	9200
CVEs:	CVE-2026-114938
Requests per second:	-
Scan CISA KEV only:	-
Fast mode:	-