网络安全预警通报

2026 年第 12 期（总第 70 期）

西安交通大学网络信息中心 2026 年 11 月 19 日

【预警类型】严重预警

【预警内容】

OpenJDK Java4Shell Base64 解码远程代码执行漏洞（CVE-2026-114938）安全预警通报

一、病毒概述

2026 年 11 月 17 日，境外安全研究机构 Calif 披露 OpenJDK Java4Shell Base64 解码远程代码执行漏洞，漏洞编号为 CVE-2026-114938。该漏洞存在于 OpenJDK 底层 Base64 解码处理路径中，属于内存越界写入漏洞。当攻击者向目标 Java 应用提交特制的 Base64 数据时，可能触发 JVM 堆内存越界写入，造成敏感信息泄露、程序崩溃甚至远程代码执行。

该漏洞主要与 OpenJDK C2 即时编译器（JIT）对 Base64 解码进行硬件加速优化有关。在支持 AVX-512 VBMI 指令集的 x86-64 处

理器上，底层汇编代码处理特定填充数据时可能出现输出长度计算下溢，导致数据写入超出目标数组边界。

经公开研究验证，Keycloak、Atlassian Jira、Atlassian Confluence、JFrog Artifactory、Jenkins、PingFederate 等产品存在预认证远程代码执行风险；Apache Kafka、Apache Solr、Elasticsearch、Gerrit、Netflix Spinnaker 等产品在认证后场景下也可能受到影响。

该漏洞具有以下特点：

（1）危害严重：攻击者可能利用内存越界写入进一步实现远程代码执行，获取服务器控制权限。

（2）影响范围广：涉及 Oracle Java SE、OpenJDK 及 Eclipse Temurin、Amazon Corretto、Azul Zulu 等多个主流 Java 发行版。

（3）攻击入口多：身份认证、文件上传、SAML 消息及网络数据解析等涉及 Base64 解码的业务场景均需重点排查。

(4)利用风险较高:漏洞技术细节及 PoC 已公开,部分常见 Java 应用已验证存在预认证攻击风险。

（5）存在平台限制：漏洞利用依赖 x86-64 处理器支持 AVX-512 VBMI 指令集，ARM64 平台不受影响。

二、病毒详情

1.技术原理

CVE-2026-114938 是 OpenJDK 底层 Base64 解码优化路径中的内存越界写入漏洞。

攻击者可通过身份认证、文件上传等业务接口提交恶意 Base64 数据，触发漏洞。在满足特定利用条件时，可能进一步实现任意内存写入及远程代码执行，最终获取目标服务器运行权限。

2. 涉及病毒详情

漏洞名称：OpenJDK Java4Shell Base64 解码远程代码执行漏洞

漏洞编号：CVE-2026-114938

漏洞类型：内存越界写入（Out-of-Bounds Write）

漏洞组件：OpenJDK JVM Base64 解码模块

威胁等级：严重（Critical）

影响平台：支持 AVX-512 VBMI 指令集的 x86-64 平台

攻击方式：远程提交恶意 Base64 数据

身份认证：部分场景无需认证

主要危害：敏感信息泄露、拒绝服务、远程代码执行及服务器控制权限

主要受影响版本：

（1）Oracle JDK 17：受影响，建议升级至 17.0.21.1 及以上版本。

（2）Oracle JDK 21：受影响，建议升级至 21.0.13.1 及以上版本。

（3）Oracle JDK 25：受影响，建议升级至 25.0.5.1 及以上版本。

（4）Oracle JDK 27：受影响，建议升级至 27.0.1.1 及以上版本。

（5）JDK 8 企业性能版：8u511b33-perf 版本受影响。

（6）JDK 8 标准版、JDK 11 标准版：不受影响。

此外，Eclipse Temurin、Amazon Corretto、Microsoft Build of OpenJDK、Azul Zulu、BellSoft Liberica、SAP SapMachine 等下游发行版也需重点排查，具体影响版本以各厂商官方公告为准。

3、主要识别特征

根据公开披露的信息，发现以下情况时应提高警惕：

（1）服务器运行受影响版本的 OpenJDK 或 Oracle JDK。

（2）服务器使用支持 AVX-512 VBMI 指令集的 x86-64 处理器。

（3）业务系统存在 Base64 解码处理逻辑，尤其涉及身份认证、文件上传及数据解析等场景。

（4）服务器部署 Keycloak、Jenkins、Jira、Confluence、Kafka、Solr、Elasticsearch 等 Java 应用。

（5）应用出现异常堆内存错误、JVM 崩溃或服务异常退出等情况。

三、漏洞影响范围

1. 影响范围

该漏洞主要影响使用受影响版本 JDK 且满足相关硬件条件的 Java 应用，涉及 Oracle Java SE、OpenJDK 及多个主流下游发行版。

已验证存在风险的产品包括：

（1）Keycloak。

（2）Jenkins。

（3）Atlassian Jira。

（4）Atlassian Confluence。

（5）JFrog Artifactory。

（6）PingFederate。

（7）Apache Kafka。

（8）Apache Solr。

（9）Elasticsearch。

（10）Gerrit、Netflix Spinnaker。

此外，基于 Spring Boot、Apache Struts 开发的 Java 业务系统也需重点排查。

2. 威胁严重性

攻击者利用该漏洞可能实现远程代码执行，获取服务器运行权限，进一步造成业务数据泄露、系统服务中断及内部网络横向攻击，威胁程度较高。

四、处置建议

1.开展资产排查。全面梳理 Java 服务器及业务系统，重点核查 JDK 发行版、版本号、CPU 架构及硬件指令集支持情况，优先排查对公网开放的 Java 应用及容器环境。

2.及时升级修复。将受影响 JDK 升级至官方修复版本，其他发行版以厂商安全公告为准。升级后重启 Java 进程，确保补丁生效。

3.采取临时缓解措施。暂时无法升级的 x86-64 环境，可通过 JVM 启动参数 -XX:-UseBASE64Intrinsics 关闭 Base64 硬件加速，或使用 -XX:UseAVX=2 限制 AVX-512 执行路径。ARM64 环境不适用 -XX:UseAVX=2 参数。

4.加强安全防护。限制互联网对 Java 管理接口、身份认证接口及文件上传接口的访问，加强网络隔离和访问控制。