WhiteDefender

엔드포인트 랜섬웨어 대응 플랫폼

Security Advisory | 2026.11

Java 보안 취약점 분석 및 대응 가이드

CVE-2026-114938 (Java4Shell)

주요 영향 범위와 보안 점검·조치 방안

엔드포인트 보안 전문 기업 | EVERYZONE

ⓒ 2026 WhiteDefender

SECURITY ADVISORY

Java 원격 코드 실행 취약점 (CVE-2026-114938) 보안 권고

Oracle 2026년 11월 Critical Security Patch Update 관련

작성 기준일	2026년 11월 19일
주요 취약점	CVE-2026-114938 (공개 명칭: Java4Shell)
관련 취약점	CVE-2026-86144, CVE-2026-114939, CVE-2026-114940, CVE-2026-114941, CVE-2026-114942
근거 자료	KISA 보호나라, Oracle, OpenJDK, NIST NVD, Calif, Red Hat, 미국 CISA 공개 자료 (6장 참고문헌)

목 차

요약 3

1. 영향 여부 확인 4
   1.1 Oracle 제품 4
   1.2 OpenJDK 및 OpenJDK 기반 배포판 5
   1.3 하드웨어 조건 5
   1.4 확인 방법 6

2. 대응 방안 7
   2.1 보안 업데이트 적용 7
   2.2 임시 완화 조치 8
   2.3 단계별 대응 절차 8

3. 취약점 상세 9
   3.1 취약점 정보 9
   3.2 심각도 평가 9
   3.3 발생 원인 9

4. 공격 영향 10
   4.1 발견자 시험 결과 10
   4.2 공격 코드 공개 및 악용 현황 10

5. 함께 발표된 Java SE 취약점 11

6. 참고문헌 12

ⓒ 2026 WhiteDefender

요 약

2026년 11월 18일(한국시간) Oracle은 11월 Critical Security Patch Update(CSPU)를 통해 Java SE를 포함한 자사 제품의 신규 보안 패치 655건을 공개하였고, KISA 보호나라는 같은 날 이에 대한 보안 업데이트 권고를 게시하였다 [1][2]. 이 가운데 CVE-2026-114938은 OpenJDK Base64 디코더의 메모리 손상 취약점으로, 인증 없이 네트워크를 통해 원격 코드 실행에 이를 수 있다 [5][6]. 발견자인 Calif는 이를 'Java4Shell'이라는 이름으로 공개하였고 [5], 미국 사이버보안·인프라보안국(CISA)은 즉시 패치할 것을 강력히 권고하였다 [8].

표 1. CVE-2026-114938 핵심 정보

취약점 유형	힙 기반 버퍼 오버플로(Heap-based Buffer Overflow, 메모리 손상) [1][4]
영향 대상	OpenJDK 17.0.6 이상 및 이를 기반으로 한 배포판 [5][7] Oracle Java SE 17·21·25·27, Java SE 8 perf 빌드(8u511b33-perf), Oracle GraalVM [2]
영향 조건	AVX-512 VBMI를 지원하는 x86-64 CPU (ARM64는 해당 없음) [5][6]
공격 조건	네트워크 공격, 인증 불필요, 사용자 상호작용 불필요 [2][6]
심각도	CVSS 3.1 8.1 High (Oracle) / CVSS 4.0 9.2 Critical (Calif) / CVSS 3.0 9.8 Critical (Red Hat) [2][5][6]
패치 공개	2026년 11월 18일 06:00 (한국시간) [5]
해결 방안	공급업체별 수정 버전으로 업데이트 [1][8]. 업데이트 전까지는 JVM 옵션으로 임시 완화 [5][7]

주요 사항

- 발견자는 초기 시험에서 Keycloak, Jira, Confluence, Jenkins 등을 대상으로 기본 설정 상태에서 인증 없는 원격 코드 실행을 시연하였다고 밝혔다 [5].
- 발견자는 검증용 코드(PoC)를 공개하였으며, 제품별 공격 코드는 추후 공개할 예정이라고 밝혔다 [5].
- OpenJDK 8과 11에는 취약한 코드가 없어 영향을 받지 않는다 [3][6]. 다만 Oracle Java SE 8의 perf 빌드(8u511b33-perf)는 영향 버전에 포함된다 [2].
- 수정본 배포 시점은 공급업체와 제품에 따라 다르다. Red Hat의 경우 작성 기준일 현재 RHEL 8·9·10의 OpenJDK 패키지는 수정본이 배포되었으나, 일부 컨테이너 이미지는 아직 배포되지 않았다 [6].

권고 조치

1. 운영 중인 모든 Java 런타임(컨테이너 및 제품 내장 런타임 포함)의 버전과 서버 CPU 조건을 확인한다 [7][8].
2. 인터넷에 노출된 시스템부터 공급업체의 수정 버전을 적용한다 [1][8].
3. 즉시 업데이트할 수 없거나 수정본이 아직 없는 경우 JVM 옵션(`-XX:-UseBASE64Intrinsics`)으로 임시 완화한다 [5][7].
4. 조치 결과를 실행 중인 프로세스 단위로 확인하고, 공급업체의 후속 공지와 이상 징후를 지속적으로 확인한다 [7][8].

ⓒ 2026 WhiteDefender

1. 영향 여부 확인

Red Hat은 본 취약점이 악용되려면 표 2의 조건이 모두 충족되어야 한다고 설명하였다 [7]. 따라서 영향 여부는 Java 런타임의 버전과 서버 CPU의 지원 기능을 함께 확인하여 판단한다.

표 2. 취약점 악용 성립 조건

구분	조건
Java 버전	애플리케이션이 OpenJDK 17.0.6 이상(OpenJDK 21·25 포함)에서 실행된다.
CPU	호스트 CPU가 x86-64이며 AVX-512 VBMI 명령어 집합을 지원한다.
JVM 옵션	JVM이 `-XX:UseAVX=2` 또는 그보다 낮은 AVX 수준으로 시작되지 않았다(이 옵션은 AVX-512 명령 사용을 막는다).
입력 경로	애플리케이션이 공격자가 조작할 수 있는 Base64 데이터를 Java 표준 라이브러리의 디코더(`java.util.Base64.Decoder`)에 전달한다. HTTP Basic 인증 정보, SAML 아티팩트, CSRF 토큰, MIME 인코딩 단어 등이 대표적이며, 인증이 끝나기 전에 디코딩되는 경우가 많다.

자료: Red Hat [7]
주: ① Oracle과 OpenJDK 권고문에서는 27 계열도 영향 버전에 포함된다 [2][3].
② ARM64 시스템, AVX-512 VBMI를 지원하지 않는 x86-64 시스템, OpenJDK 8·11은 영향을 받지 않는다 [6].
③ 별도 설정이나 기본값이 아닌 기능은 필요하지 않으며, 해당 CPU에서는 가속 코드 경로가 자동으로 선택된다 [7].

Base64 디코딩은 인증, 파일 업로드 등 일반적인 기능에서도 사용되므로 [5][7], Java 버전과 CPU 조건에 해당하는 시스템은 조치 대상으로 분류할 것을 권고한다.

1.1 Oracle 제품

KISA 보호나라가 공지한 Oracle 제품별 영향 버전과 해결 버전은 표 3과 같으며, 영향 버전은 Oracle 권고문과 동일하다 [1][2].

표 3. CVE-2026-114938 영향 제품 및 해결 버전 (Oracle 제품)

제품명	영향받는 버전	해결 버전
Oracle Java SE 8 (perf 빌드)	8u511b33-perf	8u513-perf (1.8.0_513-perf-b4)
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
Oracle GraalVM for JDK	17.0.21.0.3 / 21.0.13.0.3	17.0.21.1 / 21.0.13.1
Oracle GraalVM Enterprise Edition	21.3.20.0.3	21.3.20.1

자료: KISA 보호나라 [1], Oracle [2]
주: ① 일반 Oracle Java SE 8(8u511b33)과 Java SE 11은 CVE-2026-114938의 영향 버전에 포함되지 않는다. OpenJDK 권고문에서도 본 CVE의 영향 계열은 17·21·25·27이다 [2][3].
② 영향받는 버전보다 이전 버전도 취약점의 영향이 있을 수 있으므로 해결된 버전으로 업데이트할 것을 권고한다 [1].

ⓒ 2026 WhiteDefender

1.2 OpenJDK 및 OpenJDK 기반 배포판

발견자와 Red Hat에 따르면 OpenJDK 17.0.6 이상이 영향을 받는다 [5][7]. 취약한 코드 경로는 OpenJDK 17.0.6에서 도입되었으며, OpenJDK 8과 11에는 해당 코드가 없다 [6]. 발견자는 OpenJDK로 빌드된 표 4의 배포판도 취약하다고 밝혔다 [5].

표 4. 영향받는 OpenJDK 기반 배포판

Amazon Corretto	Eclipse Temurin	Microsoft Build of OpenJDK	Azul Zulu	BellSoft Liberica
SAP SapMachine	Red Hat OpenJDK	Oracle GraalVM for JDK	Oracle Java SE	Oracle OpenJDK

자료: Calif [5]

- OpenJDK 기반 배포판은 배포판별 수정 버전을 적용해야 한다 [1]. 배포판별 공지 위치는 2.1절의 표 7을 참고한다.
- Red Hat은 RHEL 8·9·10과 Red Hat build of OpenJDK 17·21·25를 직접 영향 제품으로 안내하였으며, RHEL 기반 컨테이너 이미지와 RHEL의 패키지를 사용하는 제품도 영향을 받을 수 있다고 밝혔다 [7].
- WAS, 업무 솔루션, 어플라이언스 등 제품 안에 Java 런타임이 포함되어 배포되는 경우에는 JVM을 개별적으로 패치하지 말고 해당 제품 공급업체가 지원하는 절차에 따라 조치한다 [7].

1.3 하드웨어 조건

취약한 코드는 AVX-512 VBMI 명령을 사용하는 x86-64 전용 코드이므로, 본 취약점은 이 명령어 집합을 지원하는 CPU에서만 해당한다. ARM64 CPU는 영향을 받지 않는다 [5][6].

표 5. 하드웨어 조건에 해당하는 주요 CPU 및 클라우드 인스턴스

구분	해당 제품군
Intel Xeon	Ice Lake, Sapphire Rapids, Emerald Rapids, Granite Rapids
AMD EPYC / Ryzen	Zen 4 이상
클라우드 인스턴스(예)	AWS: C6i/M6i/R6i, C7i/M7i/R7a GCP: C3/C3D/C4/C4D/N4/N4D/M3/M4 Azure: Dsv5/Dsv6/Dasv6/Dasv7 및 관련 D 시리즈 v5~v7

자료: CPU 제품군은 Calif [5], 클라우드 인스턴스는 Red Hat [7]
주: ① 클라우드 인스턴스는 Red Hat이 영향 가능성이 높은 유형으로 예시한 것이다 [7].
② 가상화·클라우드 환경에서는 호스트 또는 가상 머신의 CPU가 AVX-512 VBMI를 지원하는지 확인해야 한다 [7].

ⓒ 2026 WhiteDefender

1.4 확인 방법

Java 버전은 다음 명령으로 확인한다.

```
# 기본 경로(PATH)의 Java 버전 확인
java -version

# 실행 중인 JVM의 버전 확인 (JDK 진단 도구 jcmd)
jcmd <PID> VM.version

# 컨테이너 내부의 Java 버전 확인
docker exec <컨테이너명> java -version
```

주: `java -version`은 기본 경로의 Java만 표시한다. 애플리케이션마다 실제로 사용하는 런타임의 공급업체와 전체 빌드 버전을 확인해야 하며, 컨테이너·제품 설치본·어플라이언스에 포함된 런타임도 확인 대상이다 [7]. Java 런타임은 소프트웨어 자산 목록에 별도 항목으로 나타나지 않을 수 있다 [8].

Linux 환경에서 CPU 조건은 다음 명령으로 확인한다.

```
# 방법 1: AVX-512 VBMI 지원 여부 확인 (Red Hat 안내)
grep -o avx512vbmi /proc/cpuinfo | head -1

# 방법 2: 관련 CPU 기능 네 가지 확인 (Calif 안내)
grep -m1 '^flags' /proc/cpuinfo | tr ' ' '\n' | grep -E '^(avx512f|avx512bw|avx512vbmi|bmi
2)$'
```

주: 방법 1은 avx512vbmi가 출력되면 해당 CPU이고, 출력이 없으면 해당하지 않는다 [7]. 방법 2는 avx512f, avx512bw, avx512vbmi, bmi2의 네 가지가 모두 출력되어야 해당한다 [5][6].

ⓒ 2026 WhiteDefender

2. 대응 방안

2.1 보안 업데이트 적용

근본적인 해결 방안은 공급업체가 배포한 수정 버전을 적용하는 것이다 [1][2]. CISA는 수정본이 제공되는 대로 적용하되 인터넷에 노출된 시스템을 우선할 것을 권고하였다 [8]. 설치 환경별 조치 방법은 표 6과 같다.

표 6. 설치 환경별 업데이트 방법

설치 환경	조치 방법
Oracle JDK / GraalVM	표 3의 해결 버전으로 업데이트 [1]
OpenJDK 기반 배포판	배포판 공급업체가 제공하는 수정 버전 적용 [1]
운영체제 패키지	운영체제 공급업체가 배포하는 OpenJDK 패키지를 최신으로 유지 [7]
컨테이너	기반 이미지가 갱신되면 컨테이너 이미지를 다시 빌드하여 배포 [7]
제품 내장 Java	JVM을 개별적으로 패치하지 않고 제품 공급업체가 지원하는 절차로 업데이트 [7]

주: Java 업데이트는 Java 프로세스(서비스)를 재시작한 후에 적용된다. 재시작 후 실행 중인 프로세스의 Java 빌드가 수정 버전인지 다시 확인한다.

표 7. OpenJDK 기반 배포판 보안 업데이트 참고 사이트

배포판	참고 사이트
Amazon Corretto	https://github.com/corretto/corretto-17/blob/develop/CHANGELOG.md https://github.com/corretto/corretto-21/blob/develop/CHANGELOG.md https://github.com/corretto/corretto-25/blob/develop/CHANGELOG.md https://github.com/corretto/corretto-27/blob/develop/CHANGELOG.md
Azul Zulu	https://docs.azul.com/core/release-notes.html
Red Hat OpenJDK	https://access.redhat.com/security/vulnerabilities/RHSB-2026-018
Eclipse Temurin	https://adoptium.net/news/2026/11/temurin-november-2026-cspu-java4shell
Microsoft OpenJDK	https://devblogs.microsoft.com/java/java-openjdk-november-2026-critical-patch-update/
Alpine	https://gitlab.alpinelinux.org/alpine/aports/-/blob/master/community/openjdk17/APKBUILD
Ubuntu	https://ubuntu.com/security/CVE-2026-114938

자료: KISA 보호나라 [1]

수정본 배포 시점은 공급업체와 제품에 따라 다르다. 예컨대 Red Hat은 작성 기준일 현재 RHEL 8의 java-17·21-openjdk, RHEL 9의 java-17·21·25-openjdk, RHEL 10의 java-21·25-openjdk 패키지에 대한 보안 권고(RHSA)를 발행하였으나, Red Hat build of Keycloak, JBoss EAP 등의 일부 컨테이너 이미지는 수정본 없이 'Affected'로 표시되어 있다 [6]. 수정본이 아직 제공되지 않은 환경에서는 2.2절의 임시 완화 조치를 먼저 적용해야 한다.

ⓒ 2026 WhiteDefender

2.2 임시 완화 조치

수정본을 즉시 적용할 수 없는 경우, 발견자와 Red Hat은 JVM을 표 8의 옵션 중 하나로 시작하여 본 취약점을 완화할 수 있다고 안내하였다 [5][7].

표 8. 임시 완화용 JVM 옵션

JVM 옵션	설명
`-XX:-UseBASE64Intrinsics`	하드웨어 가속 Base64 구현만 비활성화한다. 다른 AVX-512 최적화는 유지되며, Red Hat이 우선 권장한 옵션이다 [7].
`-XX:UseAVX=2`	AVX-512 명령 사용 전체를 비활성화한다. x86-64 환경에만 적용해야 하며, ARM64의 JVM은 이 옵션을 인식하지 못하여 시작에 실패한다 [5][7].

자료: Calif [5], Red Hat [7]
주: ① ARM64 시스템과 AVX-512 VBMI를 지원하지 않는 x86-64 시스템에는 두 옵션 모두 필요하지 않다 [7].
② 옵션은 JVM을 시작할 때 적용되므로, 설정 후 해당 Java 프로세스를 재시작해야 한다 [7].
③ 임시 조치일 뿐이므로, 수정본이 제공되면 업데이트를 적용하고 옵션을 제거한다 [7].

옵션 적용 여부는 환경 변수 설정이 아니라 실행 중인 JVM에서 직접 확인해야 한다 [7].

```
jcmd <PID> VM.flags -all | grep -F UseBASE64Intrinsics
```

주: UseBASE64Intrinsics 값이 false로 출력되어야 한다. 컨테이너에서는 docker exec, kubectl exec 등으로 내부에서 실행한다 [7].

이와 별도로 CISA는 즉시 패치가 어려운 경우의 임시 보완 통제로 애플리케이션 경계에서의 Base64 입력 제한·검증, 입력 크기 제한, 비인증 접근 제한을 제시하였다 [8]. 한편 발견자는 프록시의 요청 버퍼링이 일반적인 완화책이 되지 못한다고 밝혔다 [5].

2.3 단계별 대응 절차

CISA와 Red Hat이 권고한 조치를 순서대로 정리하면 표 9와 같다 [7][8].

표 9. 단계별 대응 절차

단계	조치 내용
① 자산 식별	소프트웨어 자산 목록에서 JDK와 Java 런타임을 확인한다. 타사 애플리케이션에 포함된 런타임, 컨테이너 이미지와 어플라이언스에 내장된 런타임도 포함한다 [8]. 애플리케이션별 런타임의 공급업체와 전체 빌드 버전을 확인한다 [7].
② 영향 판단	호스트 또는 가상 머신의 CPU가 AVX-512 VBMI를 지원하는지 확인한다 [7].
③ 우선순위 지정	인터넷에 노출된 시스템과 인증 서비스를 우선 조치한다 [7][8].
④ 업데이트	공급업체의 수정본이 제공되는 대로 적용한다 [8]. JVM을 내장한 제품은 제품 공급업체가 지원하는 절차에 따른다 [7].
⑤ 임시 완화	즉시 패치가 어려운 경우 2.2절의 임시 완화 조치를 적용하고, 수정본을 적용한 뒤 옵션을 제거한다 [7][8].
⑥ 모니터링	승인되지 않은 런타임, 예기치 않은 JVM 비정상 종료, 의심스러운 Java 프로세스 등 이상 징후를 모니터링한다 [8].

자료: CISA [8], Red Hat [7]
주: (일반 유의 사항) 긴급 변경 작업 시간과 담당자를 미리 확보하고, 이전 버전으로 되돌리는 절차를 준비하며, 적용 후 서비스 정상 동작을 확인하는 등 통상의 변경 관리 절차를 함께 따른다.

ⓒ 2026 WhiteDefender

3. 취약점 상세

3.1 취약점 정보

표 10. CVE-2026-114938 상세 정보

CVE	CVE-2026-114938 (공개 명칭: Java4Shell) [5][8]
취약점 유형	힙 기반 버퍼 오버플로(Heap-based Buffer Overflow) [1] CWE-122 (NVD, CISA-ADP 분류) [4] / CWE-787 범위 밖 쓰기(Out-of-bounds Write) (Red Hat 분류) [6]
구성요소	Oracle 분류: Compiler [2] / OpenJDK 분류: hotspot/compiler [3] 대상 기능: Base64 디코더(`java.util.Base64.Decoder`) [7]
공격 조건	네트워크 공격, 인증 불필요, 사용자 상호작용 불필요, 공격 복잡도 높음 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H [2][4]
악용 방식	웹 서비스와 같이 해당 구성요소의 API로 데이터를 전달하는 방식으로만 악용 가능 [2][4]
영향	공격에 성공하면 Oracle Java SE 및 GraalVM이 장악될 수 있음 [4] Java 프로세스 권한으로 임의 코드를 실행하거나, 인접한 힙 메모리(인증 정보, 개인 키, 세션 토큰 등)를 읽을 수 있음 [6]
발견·제보	Quang Luong (Calif.io), Albert Yang [2]
패치 공개	2026년 11월 17일 13:00 미국 태평양 시간 (= 11월 18일 06:00 한국시간) [5]

3.2 심각도 평가

본 취약점의 심각도는 평가 기관과 CVSS 버전에 따라 차이가 있다. Oracle은 공격 복잡도를 '높음'으로 보아 CVSS 3.1 기준 8.1점을 부여하였고, Red Hat은 공격 복잡도를 '낮음'으로 보아 CVSS 3.0 기준 9.8점을 부여하였다. NVD의 자체 평가는 작성 기준일 현재 제공되지 않았다 [2][4][6].

표 11. 기관별 심각도 평가

평가 기관	기준	점수	비고
Oracle (CNA)	CVSS 3.1	8.1 (High)	공격 복잡도 '높음' [2][4]
Calif (발견자)	CVSS 4.0	9.2 (Critical)	상세 벡터 미공개 [5]
Red Hat	CVSS 3.0	9.8 (Critical)	공격 복잡도 '낮음' [6]

3.3 발생 원인

OpenJDK는 Base64 디코딩 속도를 높이기 위해 x86-64 CPU의 AVX-512 VBMI 명령을 사용하는 최적화 코드(HotSpot intrinsic)를 사용한다. 이 코드는 잘못된 Base64 입력의 끝부분(패딩 문자 '=')을 처리하는 과정에서 출력 길이를 잘못 계산하며, 그 결과 할당된 배열의 끝을 넘어 메모리를 덮어쓴다. 발견자가 제시한 사례에서는 배열 끝을 넘어 62바이트가 덮어써졌다. Java는 이후 해당 입력을 거부하지만, 그 이전에 인접한 객체가 이미 손상될 수 있다 [5].

발견자는 이 메모리 손상을 이용하여 힙 메모리 내용을 유출하고 원격 코드 실행까지 연결할 수 있다고 밝혔다. 다만 범용 공격 코드는 존재하지 않으며, 애플리케이션이 Base64를 사용하는 방식에 따라 대상별로 다른 공격 과정이 필요하다고 설명하였다 [5].

ⓒ 2026 WhiteDefender

4. 공격 영향

4.1 발견자 시험 결과

발견자는 초기 시험에서 표 12의 애플리케이션을 기본 설정 상태로 두고 원격 코드 실행을 시연하였다고 밝혔다. 이 목록은 전체가 아니며, 인증·파일 업로드와 같은 일반 기능도 취약한 Base64 디코더에 도달할 수 있어 시험 대상 외의 제품도 영향을 받을 수 있다고 설명하였다 [5]. Red Hat 역시 공개된 연구에서 널리 쓰이는 여러 Java 애플리케이션을 대상으로 기본 설정 상태에서 동작하는 공격이 시연되었다고 밝혔다 [6].

표 12. 발견자가 원격 코드 실행을 시연한 애플리케이션

구분	대상 애플리케이션
인증 전 원격 코드 실행	Keycloak, Atlassian Jira, Atlassian Confluence, JFrog Artifactory, Jenkins, PingFederate
인증 후 원격 코드 실행	Apache Kafka Broker, Apache Solr, Elasticsearch, Gerrit, Spinnaker

자료: Calif [5]

주: ① 발견자는 Apache Struts, Spring Boot 등 널리 쓰이는 프레임워크로 만든 예제 애플리케이션에서도 원격 코드 실행을 시연하였다고 밝혔다 [5].

② 발견자는 다른 연구자가 공유한 클라이언트 측 공격 사례도 소개하였다. 이에 따르면 악성 서버에 TLS로 접속하는 Java 프로그램은 자체 서비스를 외부에 노출하지 않더라도 침해될 수 있다 [5].

Red Hat은 Keycloak이 인증 전에 도착하는 요청의 Base64 데이터를 디코딩하므로, 로그인을 요구하는 것만으로는 영향받는 인스턴스를 보호할 수 없다고 설명하였다 [7].

4.2 공격 코드 공개 및 악용 현황

- 발견자는 취약점 발생 여부를 확인할 수 있는 검증 코드(PoC)를 공개하였다. 제품별 공격 코드는 사용자들이 업그레이드할 시간을 갖도록 비공개로 유지하고, 추후 공개할 예정이라고 밝혔다 [5].
- 본 문서가 참고한 자료 [1]~[8]에는 작성 기준일 현재 본 취약점이 실제 공격에 악용되었다는 내용이 없다. 다만 CISA는 승인되지 않은 런타임, 예기치 않은 JVM 비정상 종료, 의심스러운 Java 프로세스 등 이상 징후를 모니터링할 것을 권고하였다 [8].
- Oracle은 이미 패치가 공개된 취약점을 노린 공격 시도가 지속적으로 보고되고 있다고 밝히며, 지원 중인 버전을 유지하고 보안 패치를 지체 없이 적용할 것을 강력히 권고하였다 [2].

ⓒ 2026 WhiteDefender

5. 함께 발표된 Java SE 취약점

KISA 보호나라는 이번 Oracle 보안 업데이트와 관련하여 표 13의 Java 취약점을 함께 안내하였다. Java SE 17·21·25·27과 GraalVM의 경우 이들 취약점의 해결 버전은 표 3과 같다 [1].

표 13. KISA 보호나라 공지 Java 관련 취약점

CVE	대상 / 구성요소	내용	CVSS 3.1
CVE-2026-114938	Java SE / Compiler	힙 기반 버퍼 오버플로	8.1
CVE-2026-86144	Java SE, JavaFX / libxml2	XML 외부 엔티티(XXE) 주입 및 SSRF	7.5
CVE-2026-114939	Java SE / JGSS	정보 노출 및 데이터 변조	7.4
CVE-2026-114940	Java SE / JSSE	정보 노출 및 데이터 변조	7.4
CVE-2026-114941	Java SE / Compiler	서비스 거부 및 데이터 변조	7.0
CVE-2026-114942	Java SE / Libraries	서비스 거부 및 데이터 변조	7.0

자료: 내용은 KISA 보호나라 [1], CVSS 점수는 Oracle 권고문 [2]
주: ① 위 취약점 중 일부는 Java SE 8 일반 빌드(8u511b33 → 8u513, 1.8.0_513-b04)와 Java SE 11(11.0.33.0.3 → 11.0.33.1)에도 해당하며, JavaFX(21.0.13.1 / 25.0.5.1 / 27.0.1.1)도 업데이트 대상이다. 버전별 상세 내용은 KISA 공지를 참고한다 [1].
② Oracle 11월 CSPU에는 Java SE 신규 보안 패치 11건을 포함하여 총 655건의 신규 보안 패치가 포함되어 있다 [2].

ⓒ 2026 WhiteDefender

6. 참고문헌

[1] 한국인터넷진흥원(KISA), 「Oracle 제품 보안 업데이트 권고」, KISA 보호나라&KrCERT/CC 보안공지, 2026.11.18 (2026.11.19 수정).
https://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000133&pageIndex=1&nttId=72313&menuNo=205020

[2] Oracle, “Oracle Critical Security Patch Update Advisory - November 2026,” 2026.11.17 (미국 기준).
https://www.oracle.com/security-alerts/cspunov2026.html

[3] OpenJDK Vulnerability Group, “OpenJDK Vulnerability Advisory: 2026/11/17,” 2026.11.17.
https://openjdk.org/groups/vulnerability/advisories/2026-11-17

[4] NIST National Vulnerability Database, “CVE-2026-114938 Detail,” 2026.11.19 최종 수정.
https://nvd.nist.gov/vuln/detail/CVE-2026-114938

[5] Calif, “Java4Shell: Write once, RCE everywhere,” 2026.11.17 (미국 기준).
https://calif.io/java4shell/

[6] Red Hat, “CVE-2026-114938,” Red Hat CVE Database, 2026.11.18 최종 수정 (UTC 기준).
https://access.redhat.com/security/cve/CVE-2026-114938

[7] Red Hat, “RHSB-2026-018 Remote Code Execution via memory corruption on x86-64 systems - OpenJDK (CVE-2026-114938),” Red Hat Security Bulletin, 2026.11.18 수정.
https://access.redhat.com/security/vulnerabilities/RHSB-2026-018

[8] CISA, “Critical Java Vulnerability Requires Immediate Patching,” Alert, 2026.11.17.
https://www.cisa.gov/news-events/alerts/2026/11/17/critical-java-vulnerability-requires-immediate-patching

주: 위 자료는 모두 2026년 11월 19일에 확인하였다. 본문에서 출처 번호가 없는 문장은 특정 자료의 내용이 아니라 일반적인 기술·운영 유의사항이다.

본 문서는 2026년 11월 19일 기준 공개 자료를 정리한 것으로, 각 기관의 후속 공지에 따라 내용이 변경될 수 있다.
문의 : 안티랜섬웨어 화이트디펜더

ⓒ 2026 WhiteDefender