[ ] Oracle Java(JSSE) (CVE-2026-91403)

[ ] Oracle Java(JSSE) (CVE-2026-91403)

1)

Java TLS (JSSE) eMudhra CA , TLS (CVSS 9.1, ·). JDK/JRE , HTTPS (MitM) . , .

2)

- () "" JDK/JRE . (, EOL)

3) ()

- Oracle Java SE: 8u511 / 11.0.33 / 17.0.21 / 21.0.13 / 25.0.5 / 27.0.1
- OpenJDK·Temurin : JDK 8 8u512, (11/17/21/25/27)
- Oracle GraalVM:

4)

- : .
- : , .

5)

- 2026-10-30, `apps/openjdk/*` (8u512, 17.0.21) .
- AUD JDK
  - 7.0.500 / 7.0.600: javax (Java EE), JDK 8 . JDK 8u512(1.8.0_512) (11/17 JDK)
  - 7.0.510 / 7.0.610: jakarta , JDK . JDK 17.0.21
  - javax (7.0.500 ·7.0.600) JDK , jakarta (7.0.510/7.0.610) .

6) CRM(https://cs.bimatrix.co.kr) (cherry@bimatrix.co.kr) .

7) URL

- NVD(CVE-2026-91403): https://nvd.nist.gov/vuln/detail/CVE-2026-91403
- Oracle : https://www.oracle.com/security-alerts/
- : https://www.boannews.com/news/articleView.html?idxno=146703