НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Эксплуатация критической уязвимости в OpenJDK (CVE-2026-114938)

ALRT-20261119.1| 19 ноября 2026 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Описание угрозы	По каналам Национального координационного центра по компьютерным инцидентам получены сведения о критической уязвимости в наборе инструментов для разработки программ OpenJDK, получившей название Java4Shell (CVE-2026-114938). Уязвимость затрагивает реализации OpenJDK, начиная с версии 17.0.6, а также производные дистрибутивы (Oracle Java SE, Amazon Corretto, Eclipse Temurin, Microsoft Build of OpenJDK, Azul Zulu и др.). Успешная эксплуатация уязвимости позволяет неаутентифицированному злоумышленнику удалённо выполнить произвольный код на уязвимом сервере. Наиболее высокому риску подвержены публично доступные Java-приложения: Keycloak, Atlassian Jira, Atlassian Confluence, Jenkins, JFrog Artifactory, а также приложения на базе Spring Boot и Apache Tomcat. Разработчик выпустил официальные исправления 17 ноября 2026 г.
Рекомендуемые меры по нейтрализации угрозы	1. Провести инвентаризацию инфраструктуры, использующей Java, обратив особое внимание на наличие публично доступных сервисов (Jira, Confluence, Jenkins, Keycloak и др.). 2. Обновить уязвимые версии OpenJDK до актуальных. 3. Проверить инфраструктуру на наличие признаков компрометации и настроить мониторинг попыток эксплуатации уязвимости. Убедиться, что на средствах защиты загружены актуальные сигнатуры.