Java4Shell Vulnerability

Date: November 18, 2026
Version: 1.0

Summary

VIAVI Solutions is aware of the recently disclosed Java4Shell vulnerability (CVE-2026-114938) affecting certain OpenJDK-based Java runtimes. VIAVI product teams are assessing potential impact across applicable products.

The issue is a vulnerability in the Java runtime, rather than a vulnerability identified in VIAVI-developed software. Products or components incorporating affected Java runtimes may be impacted under specific conditions.

The assessment is ongoing. Additional information regarding product impact and recommended mitigation, if required, will be published as it becomes available.

Vulnerability Details

Java4Shell (CVE-2026-114938) is a heap buffer overflow in the hardware-accelerated Base64 decoder in OpenJDK HotSpot. Specially crafted Base64 input may corrupt Java heap memory, potentially exposing sensitive information or enabling remote code execution. The vulnerable decoding path requires x86-64 processors supporting AVX-512 VBMI and affected Java runtimes, including OpenJDK 17.0.6 and later in the Java 17 line and affected Java 21, 25, and 27 builds. Java 8 and 11 are not affected by this specific flaw.

The vulnerability was publicly disclosed on November 17, 2026. Researchers demonstrated remote code execution in several widely used Java applications when vulnerable runtimes and hardware are present and attacker-controlled Base64 data reaches the decoder. Calif rates the issue 9.2 (Critical) under CVSS 4.0; Oracle rates it 8.1 (High) under CVSS 3.1. Oracle and OpenJDK released fixes on November 17, 2026. VIAVI is reviewing product exposure and will provide product-specific mitigation or update guidance as the assessment progresses.

References

https://calif.io/java4shell/

https://www.tenable.com/blog/java4shell-cve-2026-114938-frequently-asked-questions-about-openjdk-rce-vulnerability

https://techcommunity.microsoft.com/blog/azurenetworksecurityblog/addressing-java4shell-cve-2026-114938-upgrade-guidance-and-azure-waf-mitigations/4574305