Alert Status: ***HIGH***

Thursday, 19th November, 2026

ALERT

JAVA4SHELL (CVE-2026-114938) – HEAP-BASED BUFFER OVERFLOW IN ORACLE JAVA

The Department of Information and Communications Technology (DICT), through the National Cyber Security Center (NCSC), alerts all PNG Government departments, agencies and organisations to a high-severity vulnerability, CVE-2026-114938 (Java4Shell), affecting Oracle Java SE and Oracle GraalVM products. The vulnerability could allow an unauthenticated remote attacker to compromise vulnerable systems, potentially resulting in a complete system takeover.

Affected Products:
According to the National Vulnerability Database (NVD), the following Oracle products and versions are affected:

- Oracle Java SE: 8u511b33-perf, 17.0.21.0.3, 21.0.13.0.3, 25.0.5.0.3 and 27.0.1.0.3.
- Oracle GraalVM for JDK: 17.0.21.0.3 and 21.0.13.0.3.
- Oracle GraalVM Enterprise Edition: 21.3.20.0.3.

Vulnerability Impact:
The vulnerability is a heap-based buffer overflow (CWE-122) in Java's Base64 decoder. Successful exploitation may allow unauthenticated attackers with network access to execute arbitrary code, disclose sensitive information or compromise the confidentiality, integrity and availability of affected systems.

Exploitation is dependent on specific processor capabilities and application configurations, including the use of affected Base64 decoding functionality on supported x86-64 processors.

Mitigation:
DICT and NCSC strongly recommend that organisations:

- Identify affected Oracle Java SE and GraalVM installations across their systems and infrastructure.
- Apply the latest security updates provided by Oracle for affected products.
- Review internet-facing applications and services that process Base64-encoded data, authentication headers and security tokens.
- Monitor affected systems for suspicious activity, unexpected application crashes and potential exploitation attempts.
- Consult Oracle's official security advisory for affected versions, patching instructions and available mitigation measures.
- Organisations operating affected Java environments should prioritise vulnerability assessment and patching to reduce the risk of remote compromise, information disclosure and service disruption.

Technical References:

- NVD: https://nvd.nist.gov/vuln/detail/cve-2026-114938
- CVE: https://www.cve.org/CVERecord?id=CVE-2026-114938
- Oracle: https://www.oracle.com/security-alerts/
- Calif (Security Research): https://calif.io/java4shell
- CISA: https://www.cisa.gov/news-events/alerts/2026/11/17/critical-java-vulnerability-requires-immediate-patching

For further technical assistance or to report suspected cybersecurity incidents, contact the National Cyber Security Center on support@ncsc.gov.pg.

Issued by:
National Cyber Security Centre (NCSC)

Department of Information & Communications Technology
PO Box 784, Vision City
National Capital District, Papua New Guinea

Email: info@ncsc.gov.pg
Phone: +675 3250171

ncsc.gov.pg