An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2611180322

NCSC Advisory

Vulnerability in Oracle: Oracle GraalVM for JDK, Oracle Java SE, Oracle GraalVM Enterprise Edition

CVE-2026-114938

18th, November 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-114938

Published: 2026-11-17

Vendor: Oracle Corporation

Product: Oracle GraalVM for JDK, Oracle Java SE, Oracle GraalVM Enterprise Edition

CVSS Score[1]: 8.1

Products Affected

Product	Version
Oracle Java SE	8u511b33-perf
Oracle Java SE	17.0.21.0.3
Oracle Java SE	21.0.13.0.3
Oracle Java SE	25.0.5.0.3
Oracle Java SE	27.0.1.0.3
Oracle GraalVM for JDK	17.0.21.0.3
Oracle GraalVM for JDK	21.0.13.0.3
Oracle GraalVM Enterprise Edition	21.3.20.0.3

Impact

Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service.

[1] https://www.first.org/cvss/

Common Weakness Enumeration (CWE)[2]: CWE-122 Heap-based Buffer Overflow

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Oracle Corporation.

- https://www.cve.org/CVERecord?id=CVE-2026-114938
- https://www.oracle.com/security-alerts/cspunov2026.html
- http://www.openwall.com/lists/oss-security/2026/11/17/31
- https://calif.io/java4shell
- https://github.com/Azure/azure-functions-java-worker/issues/909
- https://github.com/chainguard-dev/cg-skills/pull/17
- https://github.com/corretto/corretto-27/blob/27.0.1.1.4/CHANGELOG.md
- https://access.redhat.com/security/cve/cve-2026-114938
- https://www.cisa.gov/news-events/alerts/2026/11/17/critical-java-vulnerability-requires-immediate-patching

[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog