ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR



Critical Vulnerabilities in Oracle Java SE and OpenJDK – Potential Remote Code Execution and Memory Corruption

TLP: CLEAR
Distribution: Public
Advisory on: Critical Vulnerabilities in Oracle Java SE and OpenJDK – Potential Remote Code Execution and Memory Corruption
Severity: CRITICAL
Vulnerability Category: Remote Code Execution / Memory Corruption
Primary CVE: CVE-2026-114938
CVSS: 9.2 (CVSS v4.0, as reported); 8.1 (CVSS v3.1, as listed by Oracle)
Affected Technology: Oracle Java SE, OpenJDK, Oracle GraalVM for JDK, Java-based enterprise applications and services
Date: 18 November 2026

Executive Summary

BGD e-GOV CIRT's Cyber Threat Intelligence (CTI) Unit is issuing this advisory to alert government organizations, financial institutions, telecommunications operators, software service providers and other relevant entities in Bangladesh about multiple critical security vulnerabilities affecting Oracle Java SE and OpenJDK.

On **17 November 2026**, Oracle released its November Critical Security Patch Update addressing **11 security vulnerabilities in Java SE**. All 11 vulnerabilities are identified as potentially remotely exploitable without authentication.

Among the vulnerabilities, **CVE-2026-114938**, publicly referred to as **Java4Shell**, affects the Java Virtual Machine's optimized Base64 decoding functionality. The vulnerability involves a heap-based memory-corruption condition in the AVX-512 accelerated execution path. An unauthenticated remote attacker may exploit the flaw by supplying specially crafted Base64 data to an affected Java application running on a compatible x86-64 processor.

Successful exploitation may result in arbitrary code execution within the context of the affected Java process, memory corruption, sensitive information disclosure or application service disruption.

The vulnerability is particularly relevant to Java-based web applications, API services, enterprise middleware, transaction-processing systems, government portals and containerized workloads.

Considering the extensive use of Java-based technologies in Bangladesh's government and financial-sector infrastructure, organizations are strongly advised to identify affected Java runtimes, priorities internet-facing systems and apply the relevant security updates.

Vulnerability Details

Oracle Java SE – November 2026 Critical Security Update

Oracle's November 17, 2026 Critical Security Patch Update addresses 11 newly reported Java SE vulnerabilities.

Key security characteristics:

- 11 new Java SE security patches.
- All 11 vulnerabilities may be remotely exploitable without authentication.
- The highest CVSS v3.1 score in the Java SE risk matrix is 8.1.
- Vulnerabilities affect multiple Java components and supported releases.
- The update also addresses vulnerabilities affecting Oracle GraalVM and JavaFX.

Affected Oracle product builds

Product	Affected versions/builds
Oracle Java SE 8	8u511b33, 8u511b33-perf
Oracle Java SE 11	11.0.33.0.3
Oracle Java SE 17	17.0.21.0.3
Oracle Java SE 21	21.0.13.0.3
Oracle Java SE 25	25.0.5.0.3
Oracle Java SE 27	27.0.1.0.3
Oracle GraalVM for JDK	17.0.21.0.3, 21.0.13.0.3
Oracle GraalVM Enterprise Edition	21.3.20.0.3
Oracle JavaFX	21.0.13, 25.0.5, 27.0.1

BGD e-GOV CIRT

These are the affected Oracle builds listed in the security update. Organizations using third-party OpenJDK distributions must also review the relevant distribution-specific advisories.

CVE-2026-114938 – Java4Shell

Attribute	Details
CVE ID	CVE-2026-114938
Common name	Java4Shell
Vulnerability type	Heap-based buffer overflow / memory corruption
CWE	CWE-122 – Heap-based Buffer Overflow
Affected component	Java Base64 decoder / HotSpot JVM intrinsic
CVSS v4.0	9.2
CVSS v3.1	8.1 (Oracle risk matrix)
Attack vector	Network
Authentication	Not required under reported conditions
Potential impact	Remote Code Execution, memory disclosure, application crash

Technical description

CVE-2026-114938 is associated with a memory-corruption vulnerability in the Java standard library's Base64 decoding implementation.

The affected functionality is associated with the `java.util.Base64.Decoder` implementation and the HotSpot JVM's optimized Base64 decoding intrinsic.

On compatible x86-64 processors, the JVM may use an AVX-512 VBMI accelerated code path to process Base64 data. Specially crafted input supplied to an application that decodes attacker-controlled Base64 data may trigger an out-of-bounds memory write in this execution path.

Because the vulnerability exists within the Java runtime rather than a specific third-party application library, multiple applications using an affected runtime may be exposed.

Conditions relevant to exposure:

- The application uses an affected Java runtime.
- The runtime executes on a compatible x86-64 processor with AVX-512 VBMI support.
- Attacker-controlled data reaches the affected Base64 decoding functionality.
- The vulnerable decoding path is selected during execution.

Reported affected environments include OpenJDK 17.0.6 and later, with additional Java releases identified in technical research. Exact applicability should be confirmed against the relevant vendor advisory and fixed-build information.

ARM64 environments and x86-64 processors without the required AVX-512 VBMI capabilities are not known to be affected by this specific execution path.

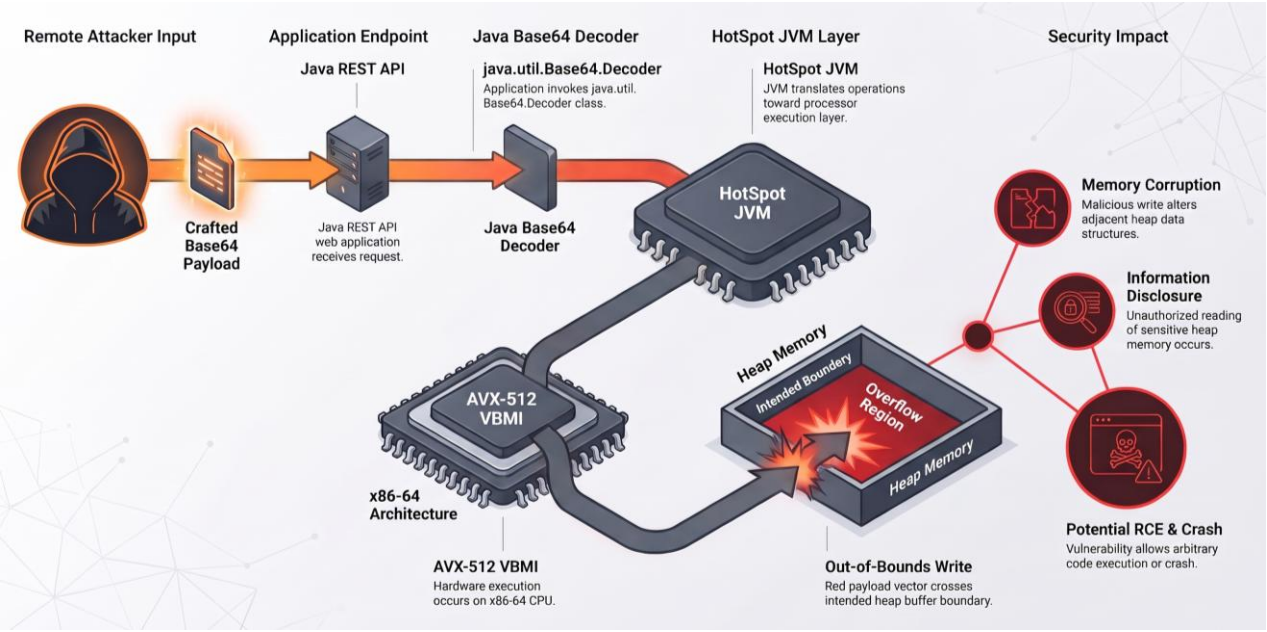


Figure: Conceptual technical representation of the reported vulnerability. Exploitability depends on the runtime, processor and application input-processing conditions

Potential consequences:

- Arbitrary code execution within the Java process context.
- Heap memory corruption and possible sensitive information disclosure.
- JVM or application process crashes.
- Unauthorized access to application-accessible resources.
- Potential compromise of connected services, depending on service privileges and network permissions.

Technical Analysis and Potential Attack Vector

Potentially Exposed Application Components

The following Java-based components should be assessed:

- Internet-facing Java web applications.
- REST APIs and backend application services.
- Java-based authentication and identity services.
- Enterprise application servers and middleware.
- Payment-processing and transaction systems.
- Document-processing and file-upload services.
- Containerized Java applications and microservices.
- Applications using Base64 decoding for authentication, token or data processing.

Base64 decoding is commonly used in application workflows involving encoded credentials, authentication artefacts, tokens and MIME-encoded data. Applications that process attacker-controlled input through the affected Java decoder require particular attention.

Potential Exploitation Sequence

BGD e-GOV CIRT

A potential exploitation scenario may involve the following stages:

- **Reconnaissance**: An attacker identifies an internet-accessible Java application or API.
- **Input delivery**: Specially crafted Base64 data is submitted to an application endpoint.
- **Decoder invocation**: The application processes the supplied data through the Java Base64 decoder.
- **Vulnerable execution**: The JVM invokes the affected optimized decoding implementation.
- **Memory corruption**: The vulnerable execution path causes an out-of-bounds memory write.
- **Code execution or disruption**: The attacker may achieve code execution within the Java process context or cause application instability.
- **Post-exploitation:** Depending on process permissions, the attacker may attempt to access application data, credentials or connected internal services.

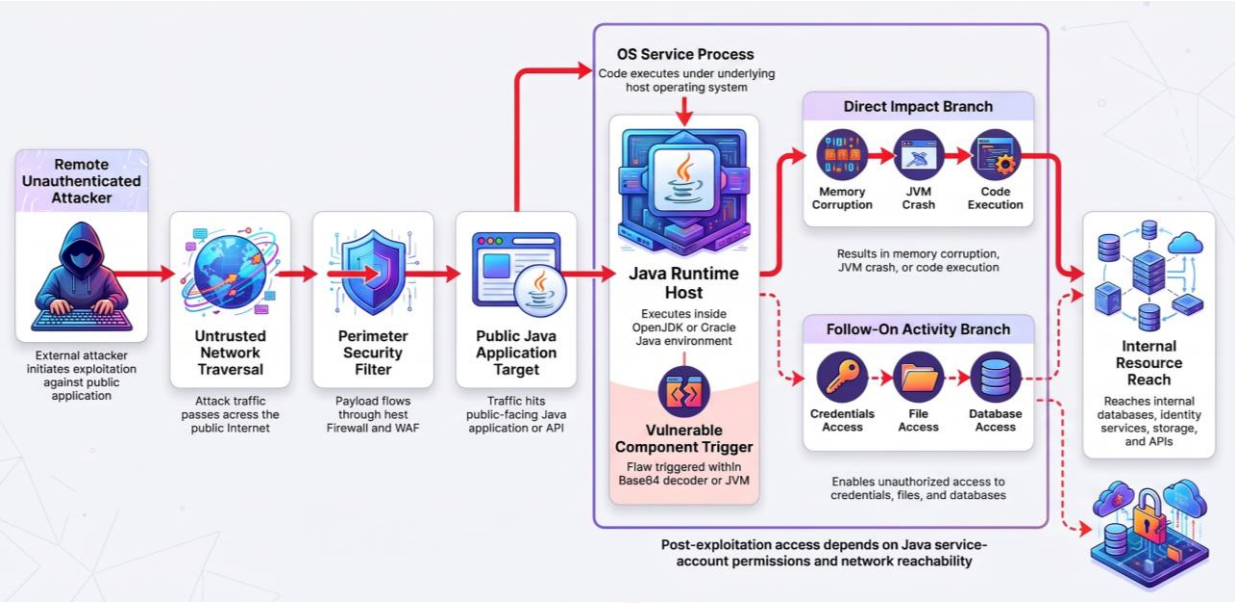


Figure: Potential Exploitation Chain Against an Internet-Facing Java Application

Potential Impact

Successful exploitation may affect the confidentiality, integrity and availability of affected systems.

Impact area	Potential consequence
Remote Code Execution	Execution of unauthorised code within the affected Java process
Confidentiality	Exposure of data accessible to the Java application
Integrity	Unauthorised modification of application data or files
Availability	JVM crash, application failure or service disruption
Credential Security	Potential exposure of application credentials, tokens or configuration
Internal Infrastructure	Potential access to connected services, depending on network and privilege controls
Business Operations	Disruption of government, banking and enterprise services

Bangladesh Threat and Exposure Assessment

Java-based applications are used across government digital services, financial platforms, enterprise systems and hosting environments. The following sectors should priorities vulnerability assessment.

Sector	Systems requiring assessment
Government and public sector	e-Government portals, citizen-service applications, backend systems and application servers
Banking and financial institutions	Internet banking, transaction-processing systems, core banking integration and API services
MFS and payment services	Payment gateways, transaction APIs and authentication services
National Data Centre and hosting	Java virtual machines, enterprise middleware, virtual machines and containers
Telecommunications	Subscriber-management systems, provisioning platforms and service APIs
Healthcare and education	Java-based information management and service platforms
Software and cloud service providers	Java application runtimes, CI/CD systems, application containers and hosted services

Bangladesh-specific assessment

Particular attention should be given to Java-based services that are:

- Accessible from the public internet.
- Connected to sensitive government or financial databases.
- Processing customer, citizen or transaction-related information.
- Running with privileged service accounts.
- Deployed in shared hosting or container environments.
- Connected to internal identity, authentication or enterprise middleware systems.

The presence of Java in an organization's infrastructure does not by itself establish vulnerability or compromise. Exposure must be confirmed through runtime, processor and application assessment.

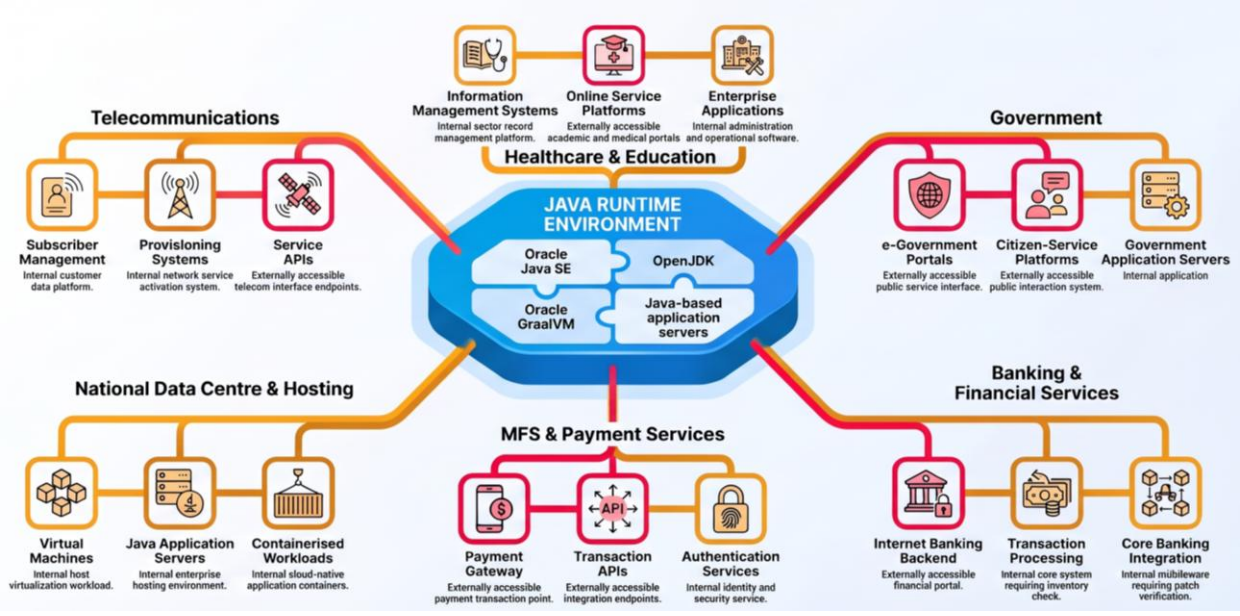


Figure: Potential Java Technology Exposure Across Bangladesh's Critical Digital Infrastructure

Detection Considerations

At the time of publication, no verified campaign-specific IP addresses, domains or file hashes have been established for CVE-2026-114938. Organizations should focus on software-version assessment and behavioral monitoring.

Host-Based Detection

Detection area	Activity to investigate
JVM logs	Fatal errors, abnormal termination and repeated crashes
Application logs	Unexpected Base64 decoding errors and malformed input processing
Process execution	Java spawning unexpected shell or system processes
File activity	Unexpected scripts, executable files or libraries created by Java
Network activity	Unusual outbound connections initiated by Java processes
Authentication logs	Unusual service-account activity following application anomalies
Container telemetry	Unexpected process execution or changes within Java application containers

Recommended SIEM Detection Logic

Rule 1 – Java spawning command interpreters

```
ParentProcessName = "java"
AND ChildProcessName IN (
"bash", "sh", "cmd.exe",
"powershell.exe", "pwsh.exe"
)
```

Rule 2 – Unexpected outbound connections

```
ProcessName = "java"
AND DestinationCategory = "External"
AND DestinationIP NOT IN ApprovedDestinationList
```

Rule 3 – Unexpected executable creation

```
ParentProcessName = "java"
AND FileExtension IN (
  ".sh", ".py", ".ps1",
  ".exe", ".dll", ".so"
)
AND FilePath NOT IN ApprovedApplicationPaths
```

Rule 4 – JVM crash monitoring

```
EventType IN (
  "JVM_FATAL_ERROR",
  "JAVA_PROCESS_CRASH",
  "APPLICATION_UNEXPECTED_TERMINATION"
)
```

These rules are behavioral detection examples. They should be tuned against approved application activity and are not unique signatures of CVE-2026-114938.

Recommended Log Sources

- Web server and reverse-proxy logs.
- WAF logs.
- Java application logs.
- JVM fatal error and crash logs.
- Linux audit and Windows Event Logs.
- EDR process and file telemetry.
- Firewall and DNS logs.
- Kubernetes audit and container logs.
- Database and authentication logs.

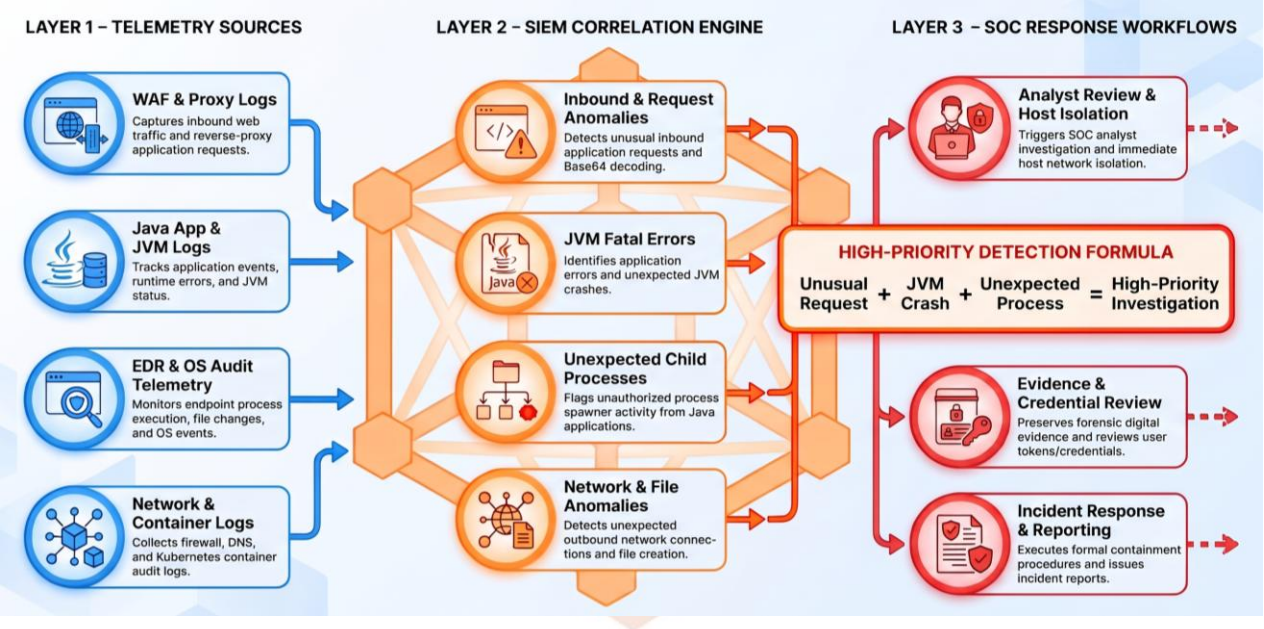


Figure: Recommended SOC Monitoring and SIEM Correlation Architecture

BGD e-GOV CIRT

Mitigation and Remediation

Recommended Fixed Versions

The November 2026 Oracle security update provides the following replacement releases:

Java release	Recommended patched version
Java SE 8	8u513
Java SE 11	11.0.33.1
Java SE 17	17.0.21.1
Java SE 21	21.0.13.1
Java SE 25	25.0.5.1
Java SE 27	27.0.1.1

For Oracle GraalVM and JavaFX, apply the corresponding fixed release identified in the Oracle security update.

Organizations using Eclipse Temurin, Red Hat OpenJDK, Amazon Corretto, Azul Zulu, Microsoft Build of OpenJDK or other distributions must apply the relevant maintainer's security update. Do not assume that Oracle's package version numbers or update schedule apply identically to every distribution.

Temporary Mitigation

Where immediate patching is not possible, the following JVM options have been reported as temporary mitigations for the affected Base64 intrinsic.

Option 1: Disable Base64 intrinsic: `-XX:-UseBASE64Intrinsics`

Option 2: Restrict AVX-512 execution: `-XX:UseAVX=2`

The second option is intended for applicable x86-64 environments. It may affect application performance and should not be applied indiscriminately to ARM systems.

Operational considerations:

- Validate the JVM option against the exact runtime distribution.
- Test in a non-production environment.
- Assess performance and application compatibility.
- Apply the setting consistently to all affected JVM instances.
- Restart services and verify that the option is active.
- Treat temporary mitigation as an interim measure, not a substitute for patching.

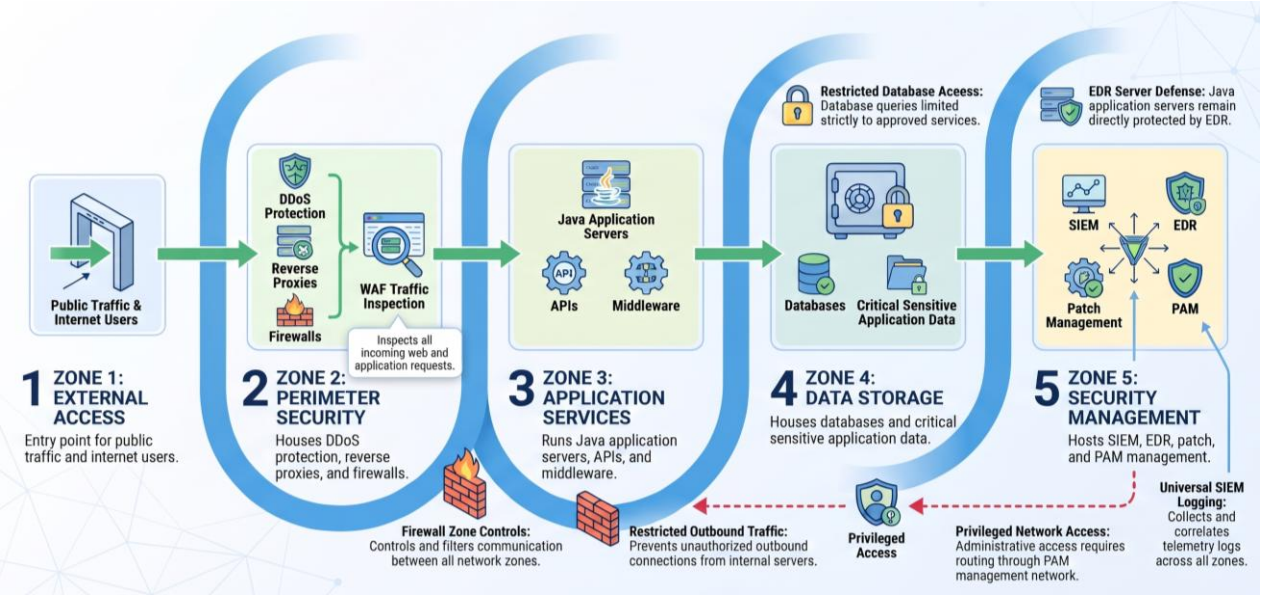


Figure: Recommended defense-in-depth architecture for Java-based government and financial application

Infrastructure Hardening

- Restrict public access to Java application and management interfaces.
- Deploy WAF and reverse-proxy controls for internet-facing services.
- Restrict unnecessary outbound connections from Java application servers.
- Segment application servers from databases and critical internal systems.
- Enforce least privilege for Java service accounts.
- Protect application secrets, environment variables and service credentials.
- Rebuild container images using patched Java runtimes.
- Review third-party software and appliances that bundle Java.
- Monitor JVM crashes, process creation and unusual network connections.

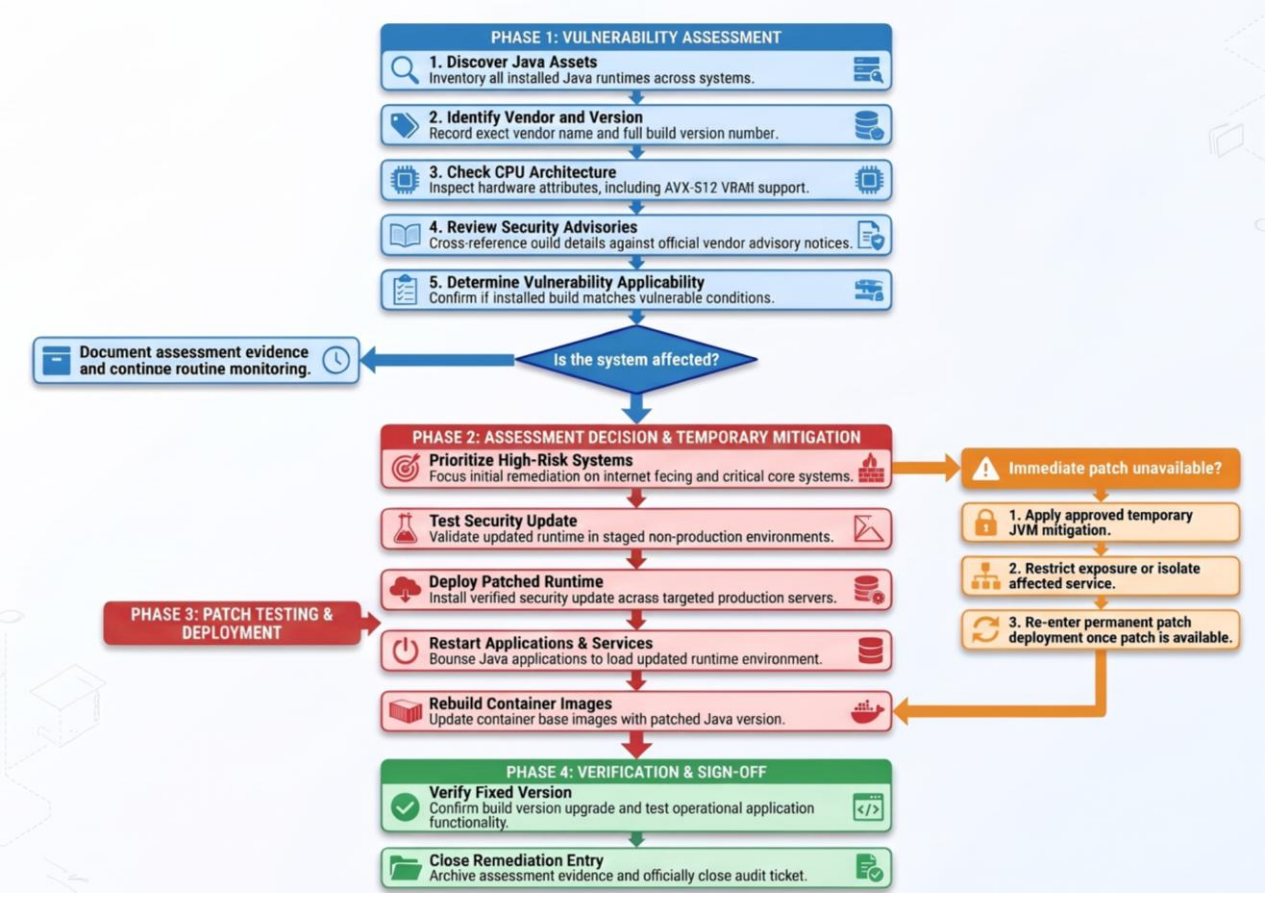


Figure: Java Vulnerability Remediation and Patch Management Workflow

Recommendations to Organizations in Bangladesh

BGD e-GOV CIRT recommends that all government organizations, financial institutions, MFS providers, telecommunications operators, hosting providers and other relevant entities:

- Conduct an immediate inventory of Oracle Java SE, OpenJDK and GraalVM installations.
- Identify Java runtimes embedded in third-party applications, appliances and container images.
- Priorities internet-facing applications and services processing externally supplied data.
- Verify processor architecture and AVX-512 VBMI capability where assessing CVE-2026-114938.
- Apply the relevant November 2026 security updates or distribution-specific patches.
- Review Java application logs, JVM crash reports and EDR telemetry for suspicious activity.
- Restrict unnecessary network access to application servers and management interfaces.
- Review service-account permissions and credentials accessible to Java processes.
- Rebuild and redeploy affected container images using patched runtimes.
- Report suspected exploitation or confirmed compromise through the appropriate organizational and national cyber incident reporting channels.

The November 2026 Oracle Java security update addresses 11 remotely exploitable Java SE vulnerabilities. Among the disclosed issues, CVE-2026-114938 presents a significant risk due to a memory-corruption condition in the Java Base64 decoding implementation that may allow unauthenticated remote code execution under applicable runtime, processor and application conditions.

Given the widespread use of Java-based systems across Bangladesh's government, financial, telecommunications and enterprise environments, organizations should urgently identify affected deployments, apply the relevant security updates and strengthen monitoring of exposed Java applications.

BGD e-GOV CIRT

BGD e-GOV CIRT's Cyber Threat Intelligence Unit recommends that all relevant organizations treat this advisory as a critical security matter and complete vulnerability assessment and remediation without unnecessary delay.

References

- https://www.oracle.com/security-alerts/cspunov2026.html
- https://thehackernews.com/2026/11/oracle-to-patch-11-java-flaws-today-as.html
- https://www.cisa.gov/news-events/alerts/2026/11/17/critical-java-vulnerability-requires-immediate-patching
- https://openjdk.org/groups/vulnerability/advisories/2026-11-17
- https://access.redhat.com/security/vulnerabilities/RHSB-2026-018
- https://www.cyber.gc.ca/en/alerts-advisories/al26-029-critical-vulnerability-impacting-oracle-java-cve-2026-114938
- https://securitylabs.datadoghq.com/articles/java4shell-remote-code-execution-in-openjdk-cve-2026-114938
- https://www.sonatype.com/blog/critical-openjdk-rce-cve-2026-114938-what-to-know

BGD e-GOV CIRT