Java4Shell OpenJDK Vulnerability

On 17 November 2026, a critical memory corruption vulnerability in the Base64 decoder of OpenJDK, known as Java4Shell (CVE-2026-114938), was publicly disclosed. OpenJDK and Oracle released fixed versions. The flaw is located in a hardware-accelerated decoding routine that the Java Virtual Machine uses on x86-64 processors supporting the AVX-512 VBMI instruction set. Crafted Base64 input can corrupt heap memory, which may lead to a crash, disclosure of process memory or remote code execution.

Based on the completed technical assessments, the dormakaba system solutions listed in this advisory use affected components. The actual exposure and required customer action depend on the individual product and are described below.

For MATRIX Cloud, dormakaba is implementing the fix. No customer action is required.

B-COMM, B-COMM 7, B-COMM HCM and the on-premises versions of MATRIX ONE and MATRIX Professional are operated by the customer and require customer action. See Section Mitigations for details.

Customers operating separate Java-based applications should assess and update those environments in accordance with the applicable vendor guidance.

Advisory Information

ID:	DKSA-26-19-111	
CVE Numbers and Scores:	CVE-2026-114938	CVSS v4.0: 9.2 (Critical)
Published:	19 November 2026	
Advisory Version:	1	

Affected Products

- B-COMM
- B-COMM 7
- B-COMM HCM
- MATRIX ONE
- MATRIX Professional
- MATRIX Cloud

Recommendation

The recommendation rating below applies to the dormakaba system solutions listed in this advisory.

Risk	Recommendation
☑ **High/Critical**	Updates should be applied as soon as possible based on organizational needs and threat model.
Medium	Within six months, based on organizational needs and threat model.
Low	During the next scheduled update cycle or within a year.
None/Info	Based on organizational needs and after appropriate testing.

Mitigations

The required actions are summarized below. See Mitigation Details in Section Vulnerability Details for further information.

- MATRIX Cloud: dormakaba is implementing the fix. No customer action is required.
- dormakaba B-COMM and B-COMM 7: Install a fixed Java version provided by the Java vendor as soon as possible.
- B-COMM HCM 2026.2: Apply the script provided by dormakaba. The fix will also be included in the next regular release.
- MATRIX ONE and MATRIX Professional: Apply the configuration change using the tool on the dormakaba Product Download portal (https://ead-download.mydormakaba.com). The fix will also be included in MATRIX 4.6.8, 4.7.6 and 4.8.2.

Customers operating separate Java-based applications or infrastructure should update to a fixed Java release from their Java vendor.

Systems with ARM-based processors or with x86-64 processors that do not support AVX-512 VBMI are not affected.

Vulnerability Details

OpenJDK is the reference implementation of the Java platform and the basis of most Java distributions, including Eclipse Temurin, Amazon Corretto, Azul Zulu, Microsoft Build of OpenJDK, Red Hat OpenJDK and Oracle Java SE. The vulnerability is located in the Java Virtual Machine and not in individual applications. Any Java application that decodes attacker-controlled Base64 data on an affected Java runtime and processor can be affected. OpenJDK and Oracle released fixed versions on 17 November 2026.

CVE-2026-114938 Out-of-Bounds Write in the OpenJDK Base64 Decoder

To accelerate Base64 decoding, the Java Virtual Machine uses a specialized routine on x86-64 processors that support the AVX-512 VBMI instruction set. When this routine processes certain malformed Base64 input with invalid padding, an internal length counter underflows and the routine writes up to 62 bytes past the end of its output buffer. This can lead to a crash, disclosure of process memory or remote code execution by an unauthenticated attacker if the affected application decodes untrusted Base64 data, for example during authentication. Systems with ARM-based processors or with processors that do not support AVX-512 VBMI are not affected.

- Classification / Type
  - CWE-191: Integer Underflow (Wrap or Wraparound)
  - CWE-787: Out-of-bounds Write
- CVSS v4.0 Base Score: 9.2 (Critical)
- Affected Versions:
  - Affected OpenJDK-based Java runtimes include OpenJDK 17 from version 17.0.6 onward and the Java 21, 25 and 27 release lines, earlier than the respective fixed versions released by the Java vendors.
  - B-COMM and B-COMM 7: All versions, when operated with an affected Java runtime on a processor that supports AVX-512 VBMI.
  - B-COMM HCM: Release 2026.2.
  - MATRIX ONE and MATRIX Professional: All versions.
  - MATRIX Cloud

Mitigation Details

- B-COMM and B-COMM 7:

  Both products use the Java runtime that the customer installs and maintains on the server. An installation is affected if it uses Java 17.0.6 or later on a server whose processor supports AVX-512 VBMI. Customers should install a fixed Java version provided by their Java vendor as soon as possible. If processor support cannot be determined, customers should assume that the installation is affected.

- B-COMM HCM:

  Release 2026.2 ships with an affected Java Development Kit. Earlier releases ship with JDK 17.0.3 and are not affected. dormakaba provides a script that fixes the vulnerability in release 2026.2. Customers should contact their dormakaba service technician to obtain and apply the script as soon as possible. The fix will also be included in the next regular release.

- MATRIX ONE and MATRIX Professional:

  The vulnerability can be fixed by a configuration change, which dormakaba strongly recommends applying as soon as possible. A tool that applies this change to MATRIX installations on Windows is available on the dormakaba Product Download portal (https://ead-download.mydormakaba.com) under the heading "CVE-2026-114938 - Java4Shell". As the tool only changes configuration settings, it works for all MATRIX versions, including versions that are no longer maintained.

  Customers sign in to the portal with their license key. If the license key is not known, it can be found in MATRIX under System > Service > Service information, in the section "Licence information" under "codeNo".

  The same fix will be included in the next regular patches for the maintained releases MATRIX 4.6.8, 4.7.6 and 4.8.2; therefore, no separate security patches are planned.

- MATRIX Cloud:

  dormakaba is implementing the fix. No customer action is required.

Additional Information

Legal Disclaimer

Please ensure that your security measures comply with relevant regulatory requirements, including privacy and notification obligations.

Terms of Use

This content is licensed under the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/). If you distribute this content, or a modified version of it, you must provide attribution to dormakaba and provide a link to the original.

Additional Resources

- https://dormakabagroup.com/en/security
- product.security@dormakaba.com
- https://ead-download.mydormakaba.com

Appendix

CVSS Scoring

Vulnerability classification has been performed using the CVSS v4.0 scoring system. The base score should be supplemented with an analysis of the affected environment (i.e., Environmental Metrics).

The CVSS scores defined in this advisory are intended to measure the severity of specific vulnerabilities and should not be used alone to assess risk.

Severity	A qualitative measure of a vulnerability within the scope of a specific system.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence (NIST SP 800-30).

Estimated Risk Scores

dormakaba qualifies identified vulnerabilities using the OWASP Risk Rating Matrix, assessing likelihood and impact to ensure a consistent, transparent, and business-relevant severity classification based on the system's standard configuration and a "typical" user's environment. This approach supports dormakaba's responsible disclosure process by communicating an estimated risk and remediation prioritization to stakeholders.