Dimensional INSIGHT®

November 18, 2026

Security Bulletin DISA-2026-05

Priority: Medium

Java4Shell – CVE-2026-114938

Dimensional Insight Security Office &
Dimensional Insight Research and Development Laboratory

Overview

On November 17, 2026, Oracle announced security vulnerabilities in the Java Virtual Machine (JVM). The most serious of these is CVE-2026-114938, nick-named "Java4Shell" by Calif, the team that discovered and wrote up the problem. Due to a bug in how the JVM decodes "base64"-encoded text on modern processors, remote code execution is possible in some circumstances.

While the immediate danger to DI customers is low in practice, we still recommend immediate mitigation of this issue via Tomcat configuration, and a later upgrade to a fixed version of the JVM when available. **These mitigations have already been applied to customer sites hosted by Dimensional Insight.**

Impact

Dimensional Insight's web applications (DivePort, Bridge, NetDiver) and DIAL are built on the Java platform, and our software installers install OpenJDK (a version of Java) as part of the Diver Platform. OpenJDK versions 21.0.13+9 (shipped with 8.0), 17.0.21+9 (shipped with 7.2), and earlier are vulnerable. If an attacker can cause the JVM to decode a provided base64-encoded string, and if the host CPU supports the AVX-512 instruction set extensions, then remote code execution is possible. All releases of OpenJDK version 11 (shipped with 7.1 and 7.0) are not vulnerable.

None of DI's web applications attempt to decode base64 before authentication. (Note that web applications using HTTP Authentication would be vulnerable, but DI's applications do not use that mechanism. If the Tomcat manager webapps are installed, note they only accept authentication attempts from localhost by default and would not be dangerous.) After authentication, the risks we have identified are situations where a malformed XLSX workbook is presented via the Upload Portlet (an optional feature) or where an attacker can cause the DivePort server-side code (not the web browser) to access an HTTPS URL under their control. The latter would typically require privileged access to DivePort's portal configuration at a minimum, or perhaps a very specific, custom workflow involving unsanitized user input.

Once our OpenJDK supplier provides fixed versions of OpenJDK, we will distribute these fixed versions in updates to our installers for Diver Platform 7.2 and 8.0.

Mitigation

In the meantime, customers should configure Tomcat to invoke the JVM with a command-line flag that disables the flawed version of the Base64 decoder: **`-XX:-UseBASE64Intrinsics`** . The JVM will then use a less optimized, but safer, version instead, with no loss of functionality.

Windows:

- Run `tomcat10w.exe` (or `tomcat9w.exe`) from the DI Tomcat bin directory (e.g. `c:\DI\Tomcat\Tomcat 10.1\bin`)
- On the Java tab, add a new line in the "Java Options" box with:

  `-XX:-UseBASE64Intrinsics`

- Click Apply, then on the first tab Stop and Start the Tomcat service. (This will disconnect all users)

Linux:

- Modify the Tomcat configuration file your OS distribution uses (such as /etc/default/tomcat10) or the tomcat systemd configuration file to add **`-XX:-UseBASE64Intrinsics`** to the JAVA_OPTS or CATALINA_OPTS environment variable. Then restart the tomcat service (this will disconnect all users).

Please contact Dimensional Insight's Customer Support if you need any assistance or have further questions.

© 2026 Dimensional Insight, Inc.