Dimensional INSIGHT

October 21, 2026

Security Bulletin DISA-2026-04

Priority: Low

eMudra Certificate Authority – weak private keys

Dimensional Insight Security Office &
Dimensional Insight Research and Development Laboratory

Overview

On October 20, 2026, eMudhra Limited, a public key infrastructure company based in India, was discovered to have issued intermediate certificates with weak private keys (such as the number "4"). A description of the issue can be found at https://emudhra.we-have-a-problem.com/. These weak certificates had put the entire digital certificate security of the web at risk. Attackers could have used these certificates to impersonate other websites, under certain conditions.

Immediately, browser manufacturers stopped trusting these certificates, mitigating most of the problems. Certain software suites, such as Java, also trust these certificates, and therefore will need to be updated. The certificate issue as it relates to Java is described in CVE-2026-114820.

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 prior to 21.0.13 trust these bad certificates.

Given that our web applications do not download code from the Internet, and only rely on these certificates in a few situations (such as contacting an AI provider), we rate the risk of this vulnerability as Low as it applies to our software. Once our OpenJDK supplier, Adoptium, provides a fixed version of OpenJDK, we will distribute this fixed version as updates to our installers.

Mitigation

In the meantime, customers who wish to mitigate the issue before then can follow the instructions here: https://openjdk.org/emudhra. We recommend the "Remove the relevant root certificates" option described on that page until we update our installers to include a fixed version of OpenJDK.

© 2026 Dimensional Insight, Inc.