

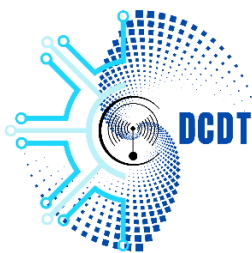
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

11 September 2026

Advisory 297: Amazon Deep Java Library Tensor Buffer Validation Integer Overflow Leading to Out-of-Bounds Memory Read (CVE-2026-85228).

Release Date: 10th September 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and developers that use Amazon Deep Java Library (DJL) to build, train, or serve machine learning models in Java applications. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-85228 is a critical integer overflow vulnerability in the tensor buffer validation logic of Amazon Deep Java Library (DJL), an AWS-affiliated, open-source, engine-agnostic deep learning framework for Java, used to build and deploy machine learning models (including model-serving deployments on AWS Lambda) without requiring separate deep-learning expertise. The flaw allows an undersized buffer to pass validation checks when a payload's declared tensor shape exceeds 32-bit signed integer limits, enabling out-of-bounds memory access. A remote, unauthenticated attacker who can submit a crafted tensor payload to a DJL-based inference endpoint can exploit this to read memory beyond the intended buffer boundary, potentially leaking sensitive information from adjacent process memory.

What are the systems affected?

The following version(s) are affected:

- Amazon Deep Java Library (Maven: ai.djl/djl), versions 0.13.0 through 0.36.0 - (Affected)
- Amazon Deep Java Library 0.37.0 and later - (Not affected, patched)

Upgrade Amazon Deep Java Library to version 0.37.0 or later. Where immediate upgrade is not possible, restrict tensor inputs to trusted sources and avoid exposing binary-mode inference endpoints to untrusted callers.

What does this mean?

Typical attack flow:

1. **Submit a crafted tensor payload to a DJL-based inference endpoint**
 - An attacker sends a specially crafted binary tensor payload, declaring a shape that exceeds 32-bit signed integer limits, to an application endpoint that passes untrusted input to DJL for inference.
2. **Trigger the integer overflow to read adjacent process memory**
 - The oversized declared shape causes an integer overflow in DJL's tensor buffer validation, allowing an undersized buffer to pass the check; the resulting out-of-bounds read can leak sensitive information from adjacent process memory.

Attack vectors:

- A network-based, unauthenticated attack against any application that accepts tensor input from external callers and passes it to a vulnerable version of DJL for inference.
- No user interaction or privileges are required.

Successful exploitation may allow attackers to:

- Read memory beyond the intended tensor buffer boundary on a system running a vulnerable version of DJL.
- Potentially leak sensitive information such as other users' data, model internals, or process secrets, residing in adjacent process memory.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay
 - Upgrade Amazon Deep Java Library to version 0.37.0 or later in every application and service that depends on it.
2. Restrict tensor input sources where patching must be delayed
3. Monitor inference endpoints for malformed tensor input

Report any suspected compromise of a Deep Java Library-based application to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-85228>
2. <https://github.com/deepjavalibrary/djl>