

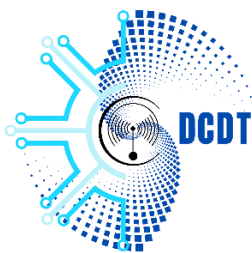
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOVERNEMENT 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

10 September 2026

**Advisory 290: eProsima Fast-DDS RTPS DATA_FRAG Out-of-Bounds Read
(CVE-2026-22590).**

Release Date: 9th 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, System/Network administrators, and engineering teams that develop or operate robotics, industrial automation, or other systems built on eProsima Fast-DDS or ROS 2 (Robot Operating System 2). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-22590 is a critical out-of-bounds read vulnerability in eProsima Fast-DDS, a widely-adopted open-source C++ implementation of the DDS (Data Distribution Service) and RTPS (Real-Time Publish-Subscribe) standards used for communication between distributed software components.

What are the systems affected?

The following version(s) are affected:

- eProsima Fast-DDS prior to 2.6.12, 2.14.6, 3.2.4, 3.3.1, or 3.4.2 (as applicable to the release line in use) - (Affected)

eProsima Fast-DDS 2.6.12, 2.14.6, 3.2.4, 3.3.1, or 3.4.2 and later - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Reach a device or system running Fast-DDS over the network**
 - An attacker with network access to a device or system using Fast-DDS for RTPS/DDS communication. For example, a robot, industrial controller, or ROS 2-based system reachable on the local network which sends a specially crafted, fragmented RTPS DATA_FRAG submessage to it.
2. **Trigger the out-of-bounds read to leak memory or crash the process**
 - Processing the malformed fragmented message causes Fast-DDS to read past the end of an allocated buffer, potentially returning sensitive heap memory contents (such as pointer values useful for defeating ASLR) to the attacker, or crashing the affected process outright.

Attack vectors:

- A network-based attack requiring no authentication or user interaction against any reachable device or system using an affected Fast-DDS version for RTPS/DDS communication.

Successful exploitation may allow attackers to:

- Leak sensitive memory contents from an affected robotics or industrial-control process, including data useful for defeating memory-protection mechanisms as a stepping stone to a more severe follow-on exploit.
- Crash the affected process, disrupting the availability of the robotics, automation, or industrial system depending on it.

Mitigation process

CERTVU recommends the following:

1. Identify every system that bundles Fast-DDS or ROS 2
 - Since Fast-DDS is typically embedded inside a larger product rather than installed as a standalone package, inventory every robotics, automation, or ROS 2-based system in your environment to determine which versions of Fast-DDS they bundle.
2. Update to a patched Fast-DDS release
3. Segment robotics and industrial-automation networks from general IT networks
4. Coordinate with equipment/robot vendors where Fast-DDS is embedded by a third party

Report any suspected compromise of a robotics, automation, or ROS 2-based system to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-22590>

2. <https://github.com/eProsima/Fast-DDS/security/advisories/GHSA-7r7h-hwfj-q626>