# Reporting Security Issues

Apache Fory™ uses the standard process outlined by the Apache Security Team for reporting vulnerabilities. Note that vulnerabilities should not be publicly disclosed until the project has responded.

To report a possible security vulnerability, please email private@fory.apache.org.

## CVE-2026-48207: PyFory ReduceSerializer DeserializationPolicy bypass

Severity: Important

Vendor: The Apache Software Foundation

Versions affected: 0.13.0 through 0.17.0 for pyfory

Description: Deserialization of untrusted data in pyfory versions 0.13.0 through 0.17.0 can bypass documented DeserializationPolicy validation in Python-native mode with `strict=False`. Applications are vulnerable when they deserialize attacker-controlled data and rely on a custom DeserializationPolicy to restrict unsafe classes, functions, or module attributes.

Mitigation: Upgrade to pyfory version 1.0.0 or later, which consistently enforces DeserializationPolicy validation for this issue. Libraries and applications that depend on Apache Fory should update their dependency requirements and release patched versions.

## CVE-2025-61622: Python RCE via unguarded pickle fallback serializer in pyfory

Severity: Critical

Vendor: The Apache Software Foundation

Versions affected: 0.5.0 through 0.12.2 for pyfory, and the legacy fury versions from 0.1.0 through 0.10.3

Description: Deserialization of untrusted data in python in pyfory versions 0.12.0 through 0.12.2, or the legacy pyfury versions from 0.1.0 through 0.10.3: allows arbitrary code execution. An application is vulnerable if it reads pyfory serialized data

from untrusted sources. An attacker can craft a data stream that selects pickle-fallback serializer during deserialization, leading to the execution of `pickle.loads`, which is vulnerable to remote code execution.

Mitigation: Users of Apache Fory are recommended to upgrade to pyfory version 0.12.3 or later, which has removed pickle fallback serializer and thus fixes this issue. Developers of libraries and applications that depend on Apache Fory should update their dependency requirements to Apache Fory 0.12.3 or later and release new versions of their software.

## CVE-2025-59328: Denial of Service (DoS) due to Deserialization of Untrusted malicious large Data

Severity: Mederate

Vendor: The Apache Software Foundation

Versions affected: 0.5.0 through 0.12.1

Description: A vulnerability in Apache Fory allows a remote attacker to cause a Denial of Service (DoS). The issue stems from the insecure deserialization of untrusted data. An attacker can supply a large, specially crafted data payload that, when processed, consumes an excessive amount of CPU resources during the deserialization process. This leads to CPU exhaustion, rendering the application or system using the Apache Fory library unresponsive and unavailable to legitimate users.

Mitigation: Users of Apache Fory are strongly advised to upgrade to version 0.12.2 or later to mitigate this vulnerability. Developers of libraries and applications that depend on Apache Fory should update their dependency requirements to Apache Fory 0.12.2 or later and release new versions of their software.