I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Bypass de políticas de deserialización
Nivel de riesgo: Alta

II. ALERTA

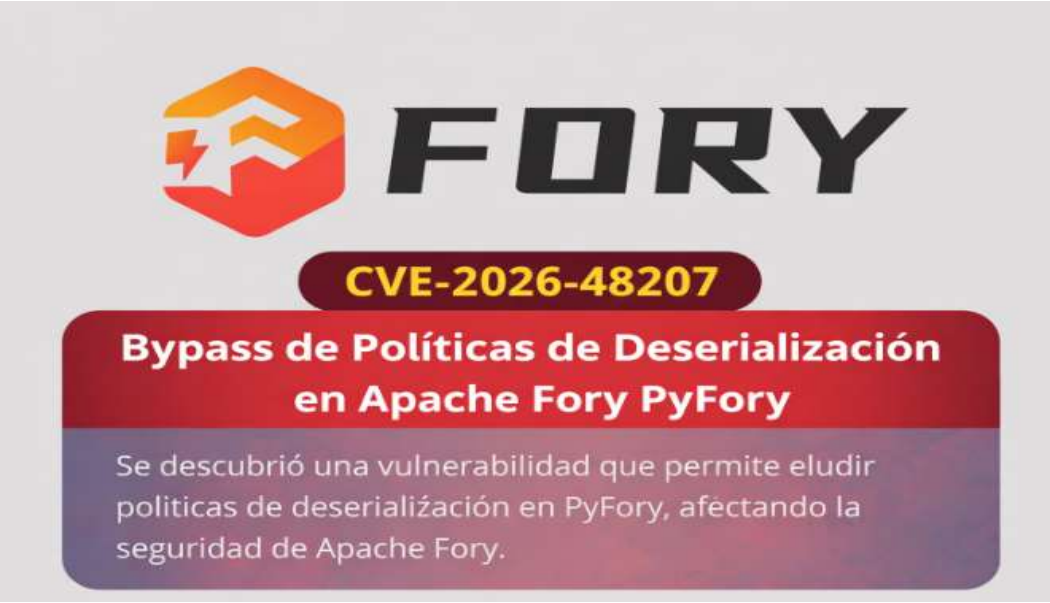

Figura 1.- CVE-2026-48207 - Bypass de Políticas de Deserialización en Apache Fory PyFory - Figura referencial

Nueva vulnerabilidad detectada denominada CVE-2026-48207 – Bypass de políticas de deserialización en Apache Fory. La vulnerabilidad reside en el módulo PyFory de Apache Fory y permite la ejecución de procesos de deserialización inseguros debido a que el componente ReduceSerializer omite la validación de la política de deserialización (DeserializationPolicy) al procesar datos controlados por un atacante. Esta vulnerabilidad podría permitir la ejecución remota de código (RCE) o provocar una denegación de servicio (DoS).

III. INTRODUCCIÓN

Apache Fory PyFory es un framework de serialización utilizados en aplicaciones Python, este framework es una herramienta o biblioteca que convierte objetos o estructuras de datos de un programa en un formato que pueda guardarse en el disco, enviarse por red, almacenarse en bases de datos o en el intercambio entre sistemas.

Consta de 2 componentes:

Componentes	Descripción
ReduceSerializer	Componente de PyFory encargado de restaurar o reconstruir objetos serializados durante el proceso de deserialización. Realiza la restauración del estado de objetos (reduce-state restoration) y la resolución de nombres globales (global-name resolution). Recibe datos serializados, interpreta cómo debe reconstruirse el objeto original, identifica las clases o funciones necesarias y vuelve a crear el objeto en memoria.
DeserializationPolicy	Mecanismo de seguridad utilizado durante la deserialización para controlar qué tipos de objetos, clases o funciones pueden reconstruirse a partir de datos serializados. Su función es prevenir que datos no confiables permitan cargar clases peligrosas, ejecutar funciones arbitrarias o reconstruir objetos maliciosos.

Tabla 1.- Componentes - CVE-2026-48207 - Bypass de Políticas de Deserialización en Apache Fory PyFory

IV. VECTOR DE ATAQUE

La vulnerabilidad CVE-2026-48207 tiene un vector de ataque tipo RED CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H con nivel de severidad 9.8 CRÍTICO.

La vulnerabilidad se origina en el componente ReduceSerializer y ocurre cuando la aplicación deserializa datos utilizando el modo nativo de Python con el modo estricto deshabilitado (strict=False), en esta configuración, durante la restauración del estado de objetos (reduce-state restoration) y la resolución de nombres globales (global-name resolution), el deserializador omite los hooks o mecanismos de validación definidos por DeserializationPolicy al procesar datos controlados por un atacante. Esto permite eludir las políticas de seguridad y posibilita la reconstrucción de objetos no confiables o peligrosos, lo que podría derivar en ejecución remota de código arbitrario (RCE) o provocar una denegación de servicio (DoS) mediante sobrecarga de CPU.

V. IMPACTO

- Apache Fory - PyFory Versiones desde 0.13.0 hasta anteriores a 1.0.0
- Componente Vulnerable ReduceSerializer

VI. INDICADORES DE COMPROMISO

- Procesamiento inesperado de objetos serializados.

- Excepciones o eventos anómalos relacionados con ReduceSerializer.
- Carga inesperada de clases o módulos Python.
- Ejecución de funciones no autorizadas durante deserialización.
- Actividad sospechosa en logs de aplicaciones backend.

VII. RECOMENDACIONES:

- Actualizar inmediatamente a Apache Fory 1.0.0 o superior.
- Habilitar strict mode en PyFory
- Evitar deserializar datos provenientes de fuentes no confiables
- Implementar validación estricta de clases permitidas
- Monitorear procesos de serialización/deserialización en aplicaciones Python
- Ejecutar servicios backend con privilegios mínimos
- Revisar aplicaciones que utilicen PyFory Python-native mode

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

APACHE FORY (2026). Security Advisories. *https://fory.apache.org/security/*

OFFSEC RADAR (2026). CVE-2026-48207 - Deserialization of Untrusted Data. *https://radar.offseq.com/threat/cve-2026-48207-cwe-502-deserialization-of-untruste-97a80f2c*

SECURITY ONLINE (2026). PyFory Deserialization Policy Bypass. *https://securityonline.info/pyfory-deserialization-policy-bypass/*

APACHE FORY (2026). Python Guide. *https://fory.apache.org/docs/guide/python/*

CVE DETAILS (2026). CVE-2026-48207. *https://www.cvedetails.com/cve/CVE-2026-48207/*