Boletín de alerta

Boletín Nro.: 49
Fecha de publicación: 29/05/2025
Tema: Alerta 2025-49 Vulnerabilidad crítica de XSS en Argo CD
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Argo CD versiones anteriores a 3.0.4.
- Versiones 2.14.0-rc1 a menores que 2.14.13.
- Versiones 2.0.0-rc3 a menores que 2.13.8.
- Versiones 1.2.0-rc1 a 1.8.7

Descripción

Se ha reportado identificó la **vulnerabilidad crítica CVE-2025-47933**, con **CVSS de 9.1**, que afecta a **Argo CD**, una herramienta de entrega continua para Kubernetes, y consiste en una falla de impropera sanitización de URLs en la página de repositorios, que permite ataques de **Cross-Site Scripting (XSS).**

El ataque XSS se lleva acabo mediante la inyección de URLs con protocolo javascript. Esto ocurre porque el código frontend no valida correctamente el protocolo de las URLs de repositorios antes de usarlas en atributos href, lo que puede ser explotado por un atacante con permisos para editar repositorios para inyectar código JavaScript malicioso. Cuando otro usuario autenticado visualiza estas URLs, el código malicioso se ejecuta en su navegador, permitiendo acciones arbitrarias en nombre de la víctima, incluyendo la creación, modificación y eliminación de recursos de Kubernetes a través de la API.

La vulnerabilidad CVE-2025-47933 compromete la seguridad operativa de entornos que utilizan Argo CD, al permitir que actores malintencionados con acceso limitado puedan escalar su influencia mediante la inyección de código malicioso en la interfaz de usuario. Esto puede resultar en la alteración de configuraciones críticas, la exposición de información sensible y la potencial interrupción de servicios gestionados en Kubernetes. La explotación efectiva de esta falla puede socavar la confianza en la plataforma y generar consecuencias graves para la continuidad y seguridad de las aplicaciones desplegadas.

Solución:

Para solucionar esta vulnerabilidad es necesario actualizar Argo CD a las versiones parcheadas que corrigen la falla de validación en la sanitización de URLs en la página siguiente https://github.com/advisories/GHSA-2hj5-g64g-fp6p.

Las versiones que incluyen el parche son la 3.0.4, 2.14.13 y 2.13.8, dependiendo de la rama que se esté utilizando. El parche introduce una validación estricta de los protocolos permitidos en las URLs, devolviendo null cuando la URL no cumple con los criterios, lo que impide la inyección de enlaces con el esquema javascript: y evita la ejecución de código malicioso en el navegador.

Medidas adicionales recomendadas incluyen:

- Se aconseja limitar los privilegios de los usuarios para que solo personal de confianza tenga permiso para editar configuraciones de repositorios, ya que la explotación requiere acceso para modificar estas URLs.
- Implementar políticas de seguridad como Content Security Policy (CSP) para restringir la ejecución de scripts en el navegador.

Monitorear continuamente la actividad y los cambios en las URLs de repositorios para detectar comportamientos sospechosos.

Argo CD Alert: XSS Flaw (CVSS 9.1) Allows Kubernetes Hijacking

Argo CD Vulnerability Let Attackers Create, Modify, & Deleting Kubernetes Resources

CVE-2025-47933 – Red Hat Customer Portal