Alerta de seguridad cibernética	9VSA23-00926-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	30 de octubre de 2023
Última revisión	30 de octubre de 2023

NOTIFICACIÓN: La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de tres nuevas vulnerabilidades de alto riesgo que afectan al controlador NGINX Ingress para Kubernetes.

Vulnerabilidades

CVE-2022-4886 CVE-2023-5043 CVE-2023-5044

Impacto

Vulnerabilidades de riesgo alto

CVE-2022-4886: Vulnerabilidad que evade la sanitización de rutas de Ingress-nginx para obtener credenciales del controlador de Ingress-nginx. CVSS: 8.8.
CVE-2023-5043: Vulnerabilidad que permite inyección de anotaciones en Ingress-nginx y ejecución arbitraria de comandos. CVSS: 7.6.
CVE-2023-5044: Inyección de código via anotación en nginx.ingress.kubernetes.io/permanent-redirect. CVSS: 7.6.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor cuando estén disponibles.

Productos afectados

NGINX Ingress Controller.

Enlaces

https://github.com/kubernetes/ingress-nginx
https://docs.nginx.com/nginx-ingress-controller/intro/overview/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4886
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5043
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5044

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.30 12:33:26 -03'00'