



Se detectan 9 vulnerabilidades en el controlador NGINX Ingress para Kubernetes

Se han revelado tres vulnerabilidades de seguridad de alta gravedad en el controlador [NGINX Ingress para Kubernetes](#) que aún no han sido corregidas y podrían ser explotadas por un actor malicioso para sustraer credenciales confidenciales del clúster.

Las debilidades se presentan de la siguiente manera:

- [CVE-2022-4886](#) (puntuación CVSS: 8.8) - La sanitización de rutas en [Ingress-nginx](#) puede ser burlada para obtener las credenciales del controlador Ingress-nginx.
- [CVE-2023-5043](#) (puntuación CVSS: 7.6) - La inyección de anotaciones en Ingress-nginx provoca la ejecución arbitraria de comandos.
- [CVE-2023-5044](#) (puntuación CVSS: 7.6) - Inyección de código a través de la anotación `nginx.ingress.kubernetes.io/permanent-redirect`.

«Estas vulnerabilidades permiten a un atacante que puede controlar la configuración del objeto Ingress robar credenciales confidenciales del clúster», [comentó](#) Ben Hirschberg, CTO y cofundador de la plataforma de seguridad de Kubernetes ARMO, en referencia a CVE-2023-5043 y CVE-2023-5044.

La explotación exitosa de estas fallas podría permitir que un adversario inyecte código no autorizado en el proceso del controlador de Ingress y obtenga acceso no autorizado a datos delicados.

CVE-2022-4886, como resultado de la falta de validación en el campo `«spec.rules[].http.paths[].path»`, posibilita que un atacante con acceso al objeto Ingress extraiga credenciales de la API de Kubernetes del controlador de Ingress.

«En el [objeto Ingress](#), el operador puede definir a qué ruta HTTP entrante se dirige la ruta interna. La aplicación vulnerable no verifica adecuadamente la validez de la ruta interna y puede apuntar al archivo interno que contiene el token de la cuenta de servicio que sirve como credencial del cliente para la autenticación contra el servidor de la API», destacó Hirschberg.



## Se detectan 9 vulnerabilidades en el controlador NGINX Ingress para Kubernetes

Ante la falta de soluciones, los mantenedores del software han lanzado medidas de mitigación que involucran habilitar la opción `«strict-validate-path-type»` y configurar la bandera `-enable-annotation-validation` para prevenir la creación de objetos Ingress con caracteres no válidos y aplicar restricciones adicionales.

ARMO indicó que la actualización de NGINX a la versión 1.19, junto con la adición de la configuración de línea de comandos `«-enable-annotation-validation»`, resuelve las vulnerabilidades CVE-2023-5043 y CVE-2023-5044.

*«A pesar de que apuntan en direcciones distintas, todas estas vulnerabilidades se originan en el mismo problema subyacente», enfatizó Hirschberg.*

*«El hecho de que los controladores de Ingress tengan acceso a secretos TLS y a la API de Kubernetes por diseño los convierte en componentes de alto privilegio. Además, dado que a menudo se enfrentan a Internet público, son muy vulnerables a la entrada de tráfico externo al clúster a través de ellos».*