Multiple Vulnerabilities in NGINX Ingress Controller

Severity Level: High

Components Affected

- NGINX prior to version 1.19

Overview

Multiple vulnerabilities have been identified in in the NGINX Ingress controller for Kubernetes that could be weaponized by a threat actor to steal secret credentials from the cluster.

Description

NGINX Ingress Controller for Kubernetes has several vulnerabilities which are described by their CVE number below:

- CVE-2022-4886 - Ingress-nginx path sanitization can be bypassed to obtain the credentials of the ingress-nginx controller.
- CVE-2023-5043 - Ingress-nginx annotation injection causes arbitrary command execution.
- CVE-2023-5044 – Code injection via nginx.ingress.kubernetes.io/permanent-redirect annotation.

Impact

- Remote Code Execution
- Security Restriction Bypass

Solution/ Workarounds

Apply fixes issued by the vendor by updating to the latest versions mentioned below:

- Update NGINX to version 1.19

Reference

- https://thehackernews.com/2023/10/urgent-new-security-flaws-discovered-in.html

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.