Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0095

Kwetsbaarheden verholpen in Kubernetes Ingress NGINX Controller

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 27-03-2025
Revisie: 1.0.1

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 1

Onderzoekers hebben Proof-of-Concept-code (PoC) gepubliceerd.

Feiten

Kubernetes heeft een aantal kwetsbaarheden in de Ingress NGINX Controller verholpen. Deze kwetsbaarheden stellen kwaadwillenden in staat een ongeauthenticeerde remote code execution (RCE) uit voeren.

Duiding

De kwetsbaarheden bevinden zich in de `ingress-nginx controller`. Deze kwetsbaarheden omvatten onder andere een kritieke remote code execution (RCE) escalatie, die verband houdt met de ingress-nginx admission controller. Een ongeauthenticeerde kwaadwillende met toegang tot het pod-netwerk kan willekeurige code uitvoeren, wat kan leiden tot de toegang van gevoelige informatie, of mogelijk zelfs overname van het cluster. Daarnaast zijn er problemen gerapporteerd met de `auth-tls-match-cn`, `mirror-target`, `mirror-host`, en `auth-url` Ingress annotaties, die allemaal kunnen leiden tot configuratie-injectie en ongeautoriseerde code-uitvoering.

Voor de duidelijkheid: De kwetsbaarheden hebben betrekking op de `Kubernetes ingress-nginx controller`. Zowel de basissoftware van Kubernetes als NginX zijn niet getroffen.

Onderzoekers hebben Proof-of-Concept-code (PoC) gepubliceerd, waarmee de kwetsbaarheden kunnen worden aangetoond. De PoC vereist Brute-forcing maar weet uiteindelijk RCE te bewerkstelligen met rechten van de applicatie. Overname van het systeem, of volledige controle lijkt niet mogelijk, maar het is aannemelijk dat er in de komende periode een toename in pogingen tot misbruik zal zijn.

Oplossingen

Kubernetes heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://kubernetes.io/blog/2025/03/24/ingress-nginx-cve-2025-1974
- https://github.com/kubernetes/kubernetes/issues/131006
- https://github.com/kubernetes/kubernetes/issues/131007
- https://github.com/kubernetes/kubernetes/issues/131008
- https://github.com/kubernetes/kubernetes/issues/131005
- https://github.com/kubernetes/kubernetes/issues/131009

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-1974	9.8 CRITICAL
CVE-2025-1097	8.8 HIGH
CVE-2025-1098	8.8 HIGH
CVE-2025-24514	8.8 HIGH
CVE-2025-24513	4.8 MEDIUM

CWE's

CWE	Beschrijving
CWE-653	Improper Isolation or Compartmentalization
CWE-20	Improper Input Validation

Getroffen producten

Kubernetes
ingress- nginx

Disclaimer