



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Tuesday, March 10, 2026

CAL-CSIC-202603-A-004

Ingress.Nginx Improper Input Validation Vulnerability

Secrets Access

Ingress Annotation

Arbitrary Code Execution

Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has identified a high severity vulnerability impacting ingress-nginx. CVE-2026-3288 carries a CVSS 3.1 score of 8.8.¹ The vulnerability is due to an improper input validation where the 'nginx.ingress.kubernetes.io/rewrite-target' Ingress annotation can be used to inject configuration into nginx. Successful exploitation can lead to arbitrary code execution in the context of the ingress.nginx controller and disclosure of Secrets accessible to the controller.² CVE-2026-3288 has not been confirmed to be exploited in the wild, and there is currently no exploit code publicly available.

A security advisory has been issued for CVE-2026-3288. A patch and workaround are included in the advisory.

The Cal-CSIC recommends immediately following the vendor's patching and upgrading guidance. If patching cannot be immediately accomplished, please follow the vendor's workaround guidance. For further information and analysis please use this link:

Security Advisory

<https://discuss.kubernetes.io/t/security-advisory-cve-2026-3288-ingress-nginx-rewrite-target-nginx-configuration-injection/34289>

Upgrade Instructions

<https://kubernetes.github.io/ingress-nginx/deploy/upgrade/>

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Products:

Affected Versions	Fixed Versions
ingress-nginx: < 1.13.8	ingress-nginx: 1.13.8
ingress-nginx: < 1.14.4	ingress-nginx: 1.14.4
ingress-nginx: < 1.15.0	ingress-nginx: 1.15.0

References

¹ NVD; “CVE-2026-3288 Detail”; <https://nvd.nist.gov/vuln/detail/CVE-2026-3288>; accessed 10 March 2026

² Kubernetes; “[Security Advisory] CVE-2026-3288: ingress-nginx rewrite-target nginx configuration injection”; <https://discuss.kubernetes.io/t/security-advisory-cve-2026-3288-ingress-nginx-rewrite-target-nginx-configuration-injection/34289>; accessed 10 March 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR