CYBER ADVISORY

Friday, February 6, 2026 **CAL-CSIC-202602-A-002**

Multiple Vulnerabilities in Kubernetes Platform

Ingress-NGINX	Arbitrary Code Execution	Patch Available	Auth-URL

The California Cybersecurity Integration Center (Cal-CSIC) has identified four vulnerabilities in the Ingress-Nginx Kubernetes gatekeeper platform that could lead to arbitrary code execution, authentication bypass, and excessive memory consumption.

CVE-2026-1580 and CVE- 2026-24512 have a high rating score of 8.8 in CVSS 3.1, and both can be used to inject configurations into nginx. Successful exploitation would lead to arbitrary code execution in the context of the ingress-nginx controller. This allows attackers to access Kubernetes Secrets available to the ingress controller which in default installations include cluster-wide Secrets.[1][2]

CVE-2026-24514 has a CVSS 3.1 score of 6.5. Attackers may use this exploit to cause memory consumption and eventually a denial-of-service condition by sending large requests to the validating admission controller – the result being the ingress-nginx controller pod being killed or the node running out of memory.[3]

CVE-2026-24513 has a CVSS 3.1 score rating of 3. Attackers can bypass the *auth-url* annotation if the ingress controller is configured with default custom errors configuration in HTTP errors 401 and 403 and if the configured default custom-errors backend is defective and fails to respect the X-Code HTTP header.[4]

The Cal-CSIC recommends immediately updating Ingress-Nginx to v1.13.7, v1.14.3, or any later version.[5] For further information refer to the Kubernetes security advisory below.

Please be advised that the Kubernetes community has scheduled the ingress-nginx project retirement for March 2026, after which no further patches or updates will be issued. [6]

Security Advisory: https://discuss.kubernetes.io/t/security-advisory-multiple-issues-in-ingress-nginx/34115

Kubernetes CVEs

CVE-ID	Severity	Description
CVE-2026-1580	8.8 High	Improper Input Validation (CWE-20) The `nginx.ingress.kubernetes.io/auth-method` Ingress annotation can be used to inject configuration into nginx.
CVE-2026-24512	8.8 High	Improper Input Validation (CWE-20) The `rules.http.paths.path` Ingress field can be used to inject configuration into nginx.
CVE-2026-24513	3.1 Low	Improper Check for Unusual or Exceptional Conditions (CWE-754) The protection afforded by the `auth-url` Ingress annotation may not be effective in the presence of a specific misconfiguration
CVE-2026-24514	6.5 Medium	Allocation of Resources Without Limits or Throttling (CWE-770) The validating admission controller feature is subject to a denial of service condition.

References

[1] Tenable; “CVE-2026-1580”; https://www.tenable.com/cve/CVE-2026-1580; accessed 5 February 2026
[2] Tenable; “CVE-2026-24512”; https://www.tenable.com/cve/CVE-2026-24512; accessed 5 February 2026
[3] Tenable; “CVE-2026-24514”; https://www.tenable.com/cve/CVE-2026-24514; accessed 5 February 2026
[4] Tenable; “CVE-2026-24513”; https://www.tenable.com/cve/CVE-2026-24513; accessed 5 February 2026
[5] Kubernetes; “ [Security Advisory] Multiple issues in ingress-nginx”; https://discuss.kubernetes.io/t/security-advisory-multiple-issues-in-ingress-nginx/34115; accessed 5 February 2026
[6] Kubernetes; “Ingress NGINX Retirement: What You Need to Know”; https://kubernetes.io/blog/2025/11/11/ingress-nginx-retirement/; accessed 5 February 2026