CYBER ADVISORY

Monday, July 13, 2026 **CAL-CSIC-202607-A-006**

Critical Argument Injection Vulnerability Contained Within MCP Server Kubernetes

Unauthorized Access	Potential Lateral Movement	Cluster Compromise	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critically rated vulnerability contained within MCP Server Kubernetes. The specialized software component acts like a bridge, allowing AI assistants or other automated tools to interact with Kubernetes clusters. By providing structured tools for common tasks like fetching, describing, or deleting cluster resources, it enables AI systems to execute operational commands directly on the infrastructure.[1] CVE-2026-61459 is an argument injection vulnerability that carries a CVSS 3.1 score of 9.8.[2]

CVE-2026-61459 is a vulnerability that stems from how certain command-line tools handle parameters. If the MCP server is exposed externally, it allows the attacker to steal credentials by sending specially crafted requests to the server. A successful compromise allows the attacker to bypass security checks and inject malicious arguments that would lead to the compromise of the entire Kubernetes cluster by transmitting sensitive authentication tokens, unauthorized access to all the resources in the targeted cluster, and potential lateral movement across multiple clusters if shared credentials exist.[3]

The developer has acknowledged this vulnerability and has issued an update that will patch CVE-2026-61459.[4]

The Cal-CSIC recommends following the developer's update guidance as soon as possible. For additional CVE details for CVE-2026-61459, please use this link:

Patch Link: https://github.com/Flux159/mcp-server-kubernetes/releases/tag/3.9.0

Additional CVE Details: https://github.com/alan-turing-institute/cyber-threat-observatory/blob/main/reports/2026-07-10/TIER_2_CVE-2026-61459.md

Affected Product and Version

Product	Affected Version
MCP Server Kubernetes	All versions prior to 3.9.0

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] Halo Security; "MCP Server Kubernetes Argument Injection Allows Cluster Compromise"; https://cve.halosecurity.com/cve-advisory/cve-2026-61459-mcp-server-kubernetes-argument-injection-leading-to-cluster; accessed 13 July 2026

[2] OpenCVE; "CVE-2026-61459"; https://app.opencve.io/cve/CVE-2026-61459; accessed 13 July 2026

[3] Halo Security; "MCP Server Kubernetes Argument Injection Allows Cluster Compromise"; https://cve.halosecurity.com/cve-advisory/cve-2026-61459-mcp-server-kubernetes-argument-injection-leading-to-cluster; accessed 13 July 2026

[4] Github; "Flux159/mcp-server-kubernetes";https://github.com/Flux159/mcp-server-kubernetes/releases/tag/3.9.0; accessed 13 July 2026