CYBER ADVISORY

TLP:CLEAR

15 March 2024

Kubernetes Windows Vulnerability

CVE-2023-5528 | Kubernetes | RCE | High Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high vulnerability known as CVE-2023-5528.[1] The vulnerability affects Kubernetes versions earlier than 1.28.4 running both on-prem deployments and Azure Kubernetes Service. Additionally, Kubernetes clusters are only affected if they are using an in-tree storage plugin for Windows nodes.[2] Exploitation of the vulnerability may allow an attacker to modify a parameter and apply 3 YAML files to execute remote code execution, RCE over the Windows endpoints and achieve full take over.[3]

The Cal-CSIC recommends immediate upgrade to Kubernetes version 1.28.4 or later if the system is running Windows nodes.

For further information on applying upgrades, please refer to Kubernetes Cluster Management.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.

Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Dark Reading; "Patch Now: Kubernetes RCE Flaw Allows Full Takeover of Windows Nodes;" https://www.darkreading.com/cloud-security/patch-now-kubernetes-flaw-allows-for-full-takeover-of-windows-nodes; accessed 15 March 2024

[2] GitHub; "CVE-2023-5528: Insufficient input sanitization in in-tree storage plugin leads to privilege escalation on Windows nodes #121879;" https://github.com/kubernetes/kubernetes/issues/121879; accessed 15 March 2024

[3] Red Hat; "https://access.redhat.com/security/cve/cve-2023-5528; accessed 15 March 2024