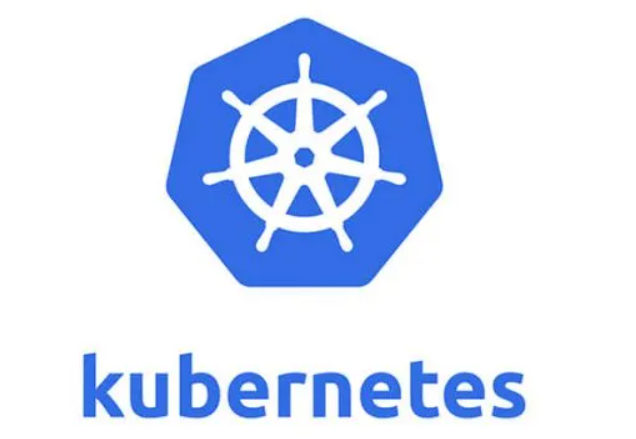
WINDOWS ENDPOINT REMOTE CODE EXECUTION COULD be caused by KUBERNETES flaws.

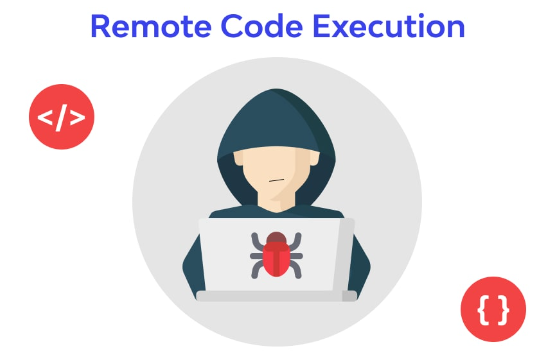


A high-severity vulnerability in Kubernetes has been identified as CVE-2023-3676 (CVSS 8.8) by Akamai researchers. Due to the detection of this problem, the two further vulnerabilities, CVE-2023-3893 and CVE-2023-3955 (CVSS 8.8), were also found. Insecure function calls and a lack of user input sanitization were the root causes of all three vulnerabilities.

On all Windows endpoints in a Kubernetes cluster, the vulnerability allows remote code execution with SYSTEM rights. Applying a malicious YAML file to the cluster will cause the problem, according to the attacker.

The flaw affects Kubernetes default installations and was tested against both on-premises and Azure Kubernetes Service deployments.

The researchers discovered that the combination of "exec.Command" and user-supplied data that had not been sanitized would have produced the right circumstances for a command injection.



Before using a value contained within a string, PowerShell users can assess it.

Any PowerShell command, such as $(Start-Process cmd), $(Invoke-Expression exp), and other PowerShell commands, can be put between the parenthesis and will be evaluated.

A YAML file's subPath subproperty can be abused by an attacker to access confidential information outside of the container. By using remote nodes to execute arbitrary commands with SYSTEM privileges (in the kubelet's own context) and take control of all Windows nodes in the cluster, the subPath evaluation vulnerability can be exploited.

"CVE-2023-3676 only needs access to a node and the ability to apply privileges, which lowers the barrier for attackers. The successful exploitation of this vulnerability will grant SYSTEM privileges to any Windows node on the machine, as we explained in this blog article. reads the warning that Akamai posted. "There is typically a higher likelihood of witnessing this attack (and related attacks) on companies due to the high effect and ease of exploitation.

For the purpose of preventing this vulnerability, Akamai released an OPA rule and a proof-of-concept YAML file.



Here is the timeframe for disclosure:

Vulnerability was reported to the Kubernetes team on July 13, 2023.

CVEs assigned by the Kubernetes team on July 19, 2023

Kubernetes issued the CVE patches on August 23, 2023.

2023-09-13 — Blog entry