Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Proof-of-Concept Released for Kubernetes Vulnerabilities Exposing Windows Nodes

Date of Publication	Admiralty Code	TA Number
September 14, 2023	A1	TA2023372

Summary

First Discovered: July 13, 2023
Affected Product: Kubernetes environments
Affected Platform: Windows
Impact: Three interconnected high-severity security vulnerabilities have been identified in Kubernetes. These vulnerabilities could potentially be exploited to achieve remote code execution with elevated privileges on Windows endpoints within a cluster. Notably, a proof of concept for this vulnerability is a YAML file that includes the execution of a PowerShell command, illustrating the severity of the issue.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-3676	Kubernetes Privilege Escalation Vulnerability	Kubernetes	✗	✗	✓
CVE-2023-3893	Kubernetes Privilege Escalation Vulnerability	Kubernetes	✗	✗	✓
CVE-2023-3955	Kubernetes Command Execution Vulnerability	Kubernetes	✗	✗	✓

Vulnerability Details

#1 Kubernetes has been found to possess three interconnected, high-severity security flaws. These vulnerabilities potentially allow remote code execution with root privileges on Windows endpoints within a cluster. A proof of concept for these vulnerabilities became available 22 days after the patch release. This proof of concept essentially consists of a YAML file that incorporates the execution of a PowerShell command.

#2 The three vulnerabilities, namely CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955, affect all Kubernetes environments that utilize Windows nodes. To exploit this vulnerability, an attacker would need to introduce a malicious YAML file into the cluster.

#3 The CVE-2023-3676 enables a remote user to elevate privileges on Windows nodes within Kubernetes. This vulnerability arises from inadequate input validation. An attacker with the capability to create pods on Windows nodes remotely can acquire administrative privileges on these nodes. This vulnerability permits an attacker with 'apply' privileges, granting interaction with the Kubernetes API, to inject arbitrary code. This code would then be executed on remote Windows machines with SYSTEM-level privileges, effectively compromising their security.

#4 The CVE-2023-3955 vulnerability involves a problem with input sanitization. It allows a specially crafted path string to be interpreted as a parameter to a PowerShell command, effectively leading to command execution. This flaw could be exploited to execute arbitrary commands, posing a serious security risk.

#5 CVE-2023-3893 is a vulnerability related to privilege escalation within the Container Storage Interface (CSI) proxy. This flaw permits a malicious actor to potentially gain administrator-level access on the affected node.

#6 Kubernetes has issued patches to rectify these vulnerabilities. By promptly applying these patches and ensuring that the systems are kept up to date, users can bolster their security posture and protect their infrastructure from potential attacks by malicious actors.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-3676	kubelet earlier to v1.28.1, kubelet earlier to v1.27.5, kubelet earlier to v1.26.8, kubelet earlier to v1.25.13, kubelet earlier to v1.24.17	cpe:2.3:a:kubernetes:kubernetes:-:*:*:*:*:*:*:*	CWE-20
CVE-2023-3893	kubernetes-csi-proxy earlier to v2.0.0-alpha.0, kubernetes-csi-proxy earlier to v1.1.2	cpe:2.3:a:kubernetes:csi_proxy:-:*:*:*:*:kubernetes:*:*	CWE-20
CVE-2023-3955	kubelet earlier to v1.28.1, kubelet earlier to v1.27.5, kubelet earlier to v1.26.8, kubelet earlier to v1.25.13, kubelet earlier to v1.24.17	cpe:2.3:a:kubernetes:kubernetes:-:*:*:*:*:*:*:*	CWE-20

Recommendations

Apply Patch: Install the security patch provided by Kubernetes to address the CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent vulnerabilities from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**T1609** Container Administration Command
T1610 Deploy Container	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1548** Abuse Elevation Control Mechanism
T1068 Exploitation for Privilege Escalation			

Patch Details

To address these vulnerabilities, it's essential to apply the following updates for the fixed versions:
kubelet v1.28.1
kubelet v1.27.5
kubelet v1.26.8
kubelet v1.25.13
kubelet v1.24.17
kubernetes-csi-proxy v2.0.0-alpha.1
kubernetes-csi-proxy v1.1.3

Link:
https://kubernetes.io/releases/patch-releases/

References

https://discuss.kubernetes.io/t/security-advisory-cve-2023-3676-insufficient-input-sanitization-on-windows-nodes-leads-to-privilege-escalation/25204

https://discuss.kubernetes.io/t/security-advisory-cve-2023-3893-insufficient-input-sanitization-on-kubernetes-csi-proxy-leads-to-privilege-escalation/25206

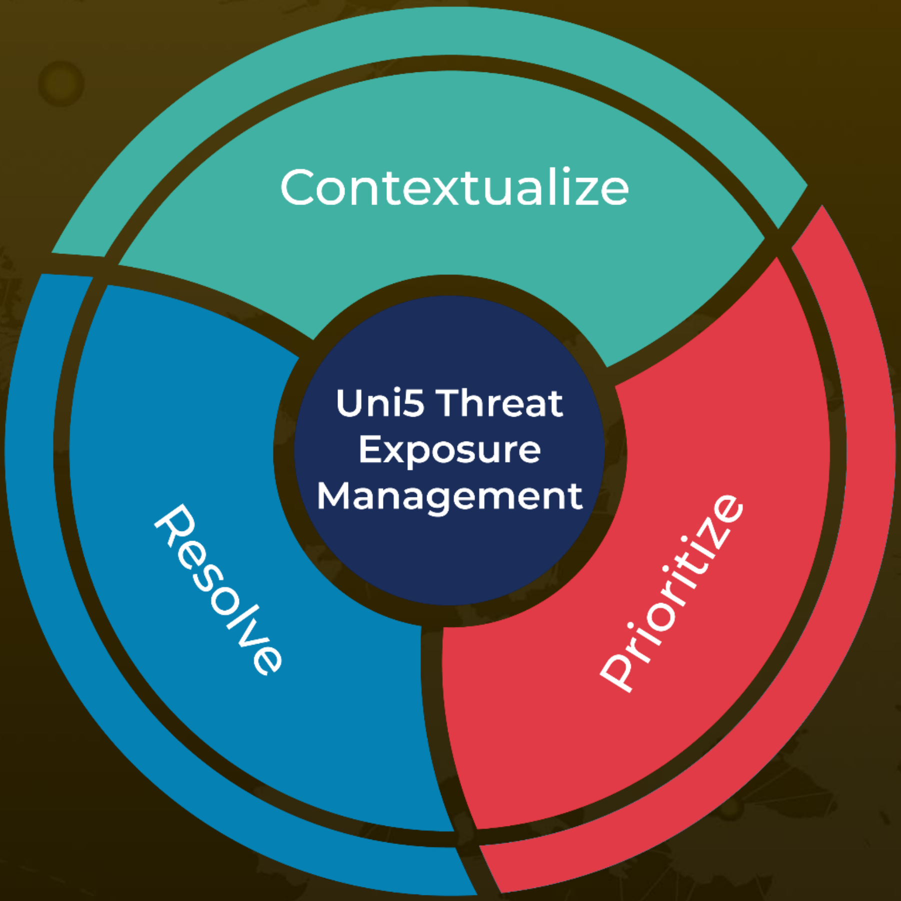
https://discuss.kubernetes.io/t/security-advisory-cve-2023-3955-insufficient-input-sanitization-on-windows-nodes-leads-to-privilege-escalation/25205

https://www.akamai.com/blog/security-research/kubernetes-critical-vulnerability-command-injection

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 14, 2023 • 6:35 AM

More at www.hivepro.com