Hive Pro

THREAT ADVISORY

Attackers Escape Kubernetes Containers using "cr8escape" Vulnerability in CRI-O

TA2022063

Threat Level RED

Publish Date – March 17, 2022

A flaw in CRI-O, an open-source Linux implementation of Kubernetes' Container Runtime Interface (CRI), was discovered that may allow an attacker to gain remote control of servers and potentially poison the container with attack code.

The "cr8escape" vulnerability (CVE-2022-0811) allows an attacker to circumvent the host's defenses and set arbitrary kernel parameters. As a result, attackers with permissions to deploy a pod on a Kubernetes cluster using the CRI-O runtime can exploit the "kernel.core_pattern" parameter to accomplish container escape and run arbitrary code as root on any node in the cluster. This allows an attacker to carry out a range of operations on targets, including malware execution, data exfiltration, and lateral movement across pods.

The vulnerability has been patched in CRI-O versions 1.19.6, 1.20.7, 1.21.6, 1.22.3, 1.23.2, 1.24.0.

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
TA0002: Execution
T1059: Command and Scripting Interpreter
TA0007: Discovery
T1613: Container and Resource Discovery
TA0003: Persistence
TA0001: Initial Access
T1133: External Remote Services

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0811	CRI-O version 1.19 and earlier	cpe:2.3:a:kubernetes:cri-o:*:*:*:*:*:*:*:*	Arbitrary code execution in cri-o via abusing “kernel.core_pattern” kernel parameter	CWE-94

Patch Link

https://github.com/cri-o/cri-o/releases

References

https://www.crowdstrike.com/blog/cr8escape-new-vulnerability-discovered-in-cri-o-container-engine-cve-2022-0811/