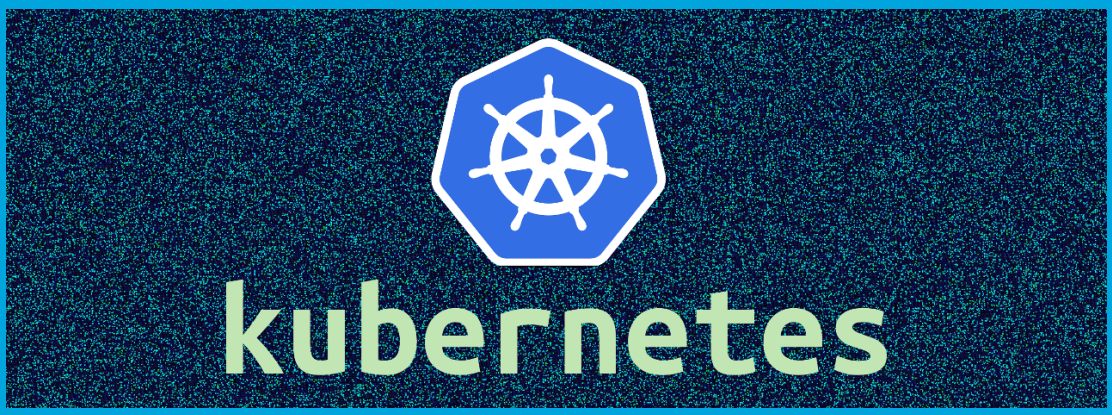
Security Newsletter

10 December 2018

Subscribe to this newsletter

Kubernetes Updates Patch Critical Privilege Escalation Bug



A critical vulnerability in Kubernetes open-source system for handling containerized applications can enable an attacker to gain full administrator privileges on Kubernetes compute nodes.

Kubernetes makes it easier to manage a container environment by organizing application containers into pods, nodes (physical or virtual machines) and clusters. Multiple nodes form a cluster, managed by a master that coordinates cluster-related activities like scaling, scheduling, or updating apps. Each node has an agent called Kubelet that facilitates communication with the Kubernetes master via the API. The number of nodes available in a Kubernetes system can be hundreds and even thousands.

The security bug was discovered by Darren Shepherd, co-founder of Rancher Labs company that provides Kubernetes-as-a-Service solution Rancher. Now tracked as CVE-2018-1002105, the flaw is critical, with a Common Vulnerability Scoring System (CVSS) score of 9.8 out of 10. The problem has been addressed in the latest Kubernetes revisions: v1.10.11, v1.11.5, v1.12.3, and v1.13.0-rc.1. Kubernetes releases prior to these along with the products and services based on them are affected by CVE-2018-1002105.

Read More on BleepingComputer

More on CVE-2018-1002105

More #News

- A Breach, or Just a Forced Password Reset?
- Google's Cloud Security Command Center gets beta release
- Windows 10 Security Questions Prove Easy for Attackers to Exploit
- New online service will hack printers to spew out spam
- Quora Gets Hacked – 100 Million Users Data Stolen
- Malicious sites abuse 11-year-old Firefox bug that Mozilla failed to fix
- Filter Bubble – DuckDuckGo Says Chrome Incognito Mode Does not Provide Anonymity
- WebKit Vulnerability Affects Latest Versions of Apple Safari
- Botnet of 20,000 WordPress Sites Infecting Other WordPress Sites
- Another MongoDB database exposes personal data of 66M users
- Marriott to reimburse some guests for new passports after massive data breach
- Solving 3rd Party Cybersecurity Risk
- 10 tips to combat phishing via social media platforms
- Flash zero-day exploit spotted – patch now!
- Warning! Unprivileged Linux Users With UID > INT_MAX Can Execute Any Command
- Apple killing off web passwords? Safari trials WebAuthn logins on macOS

#Tech and #Tools

- Demystifying Kubernetes CVE-2018-1002105 (and a dead simple exploit)
- WebKit-RegEx-Exploit
- HTTPS in the real world
- linikatz is a tool to attack AD on UNIX
- Jailbreaks Demystified

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us