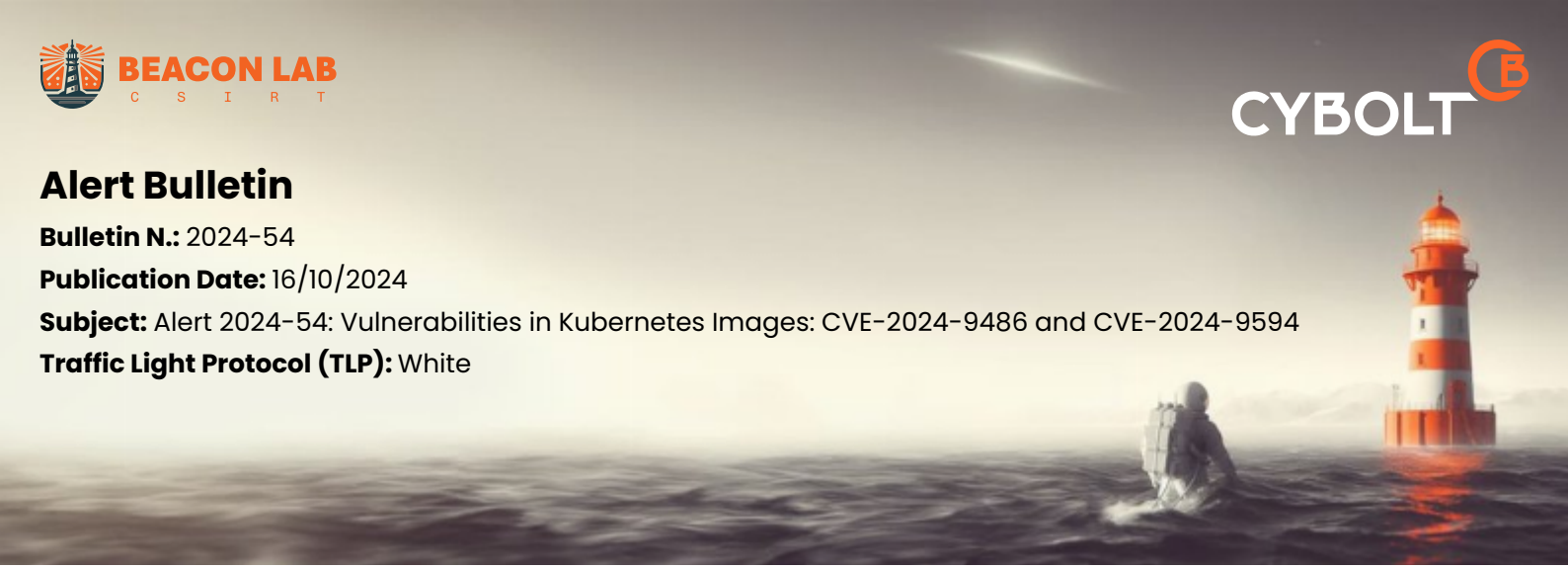

Alert Bulletin

Bulletin N.: 2024-54
Publication Date: 16/10/2024
Subject: Alert 2024-54: Vulnerabilities in Kubernetes Images: CVE-2024-9486 and CVE-2024-9594
Traffic Light Protocol (TLP): White

Description:

The vulnerabilities CVE-2024-9486 and CVE-2024-9594, identified in the image creation process in Kubernetes, are due to the use of default credentials that can expose systems to unauthorized access and manipulation.

CVE-2024-9486, with a CVSS score of 9.8, affects virtual machine images generated in Proxmox. This vulnerability stems from the failure to disable default credentials, allowing an attacker with access to them to gain full control of the system, representing a critical risk.

On the other hand, CVE-2024-9594, with a CVSS score of 6.3, impacts images created with providers like Nutanix, OVA, QEMU, and headless environments. Although the default credentials are disabled after the creation process, there is a window of risk during the image-building process.