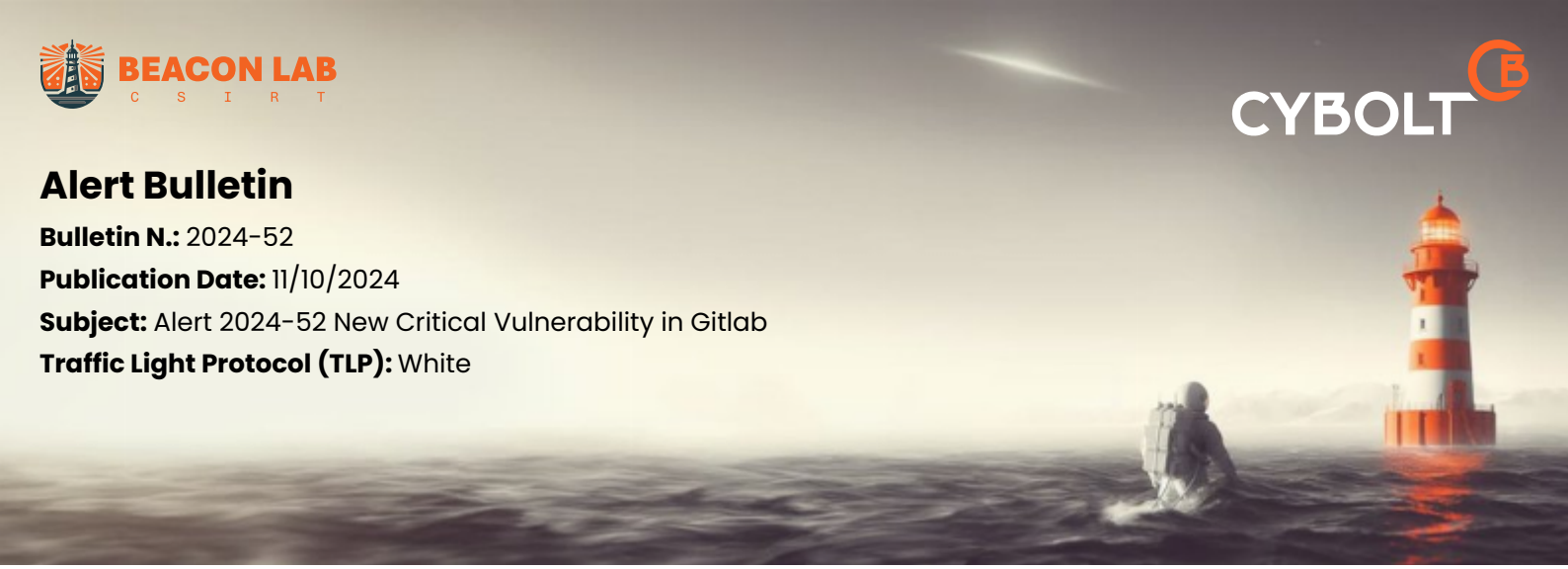

Alert Bulletin

Bulletin N.: 2024-52
Publication Date: 11/10/2024
Subject: Alert 2024-52 New Critical Vulnerability in Gitlab
Traffic Light Protocol (TLP): White

A new critical vulnerability in GitLabidentified as CVE-2024-9164has been discovered, which allows an attacker to execute pipelines with privileges of other users. This vulnerability affects versions of GitLab Enterprise Edition (EE). With a severity score of 9. 6 out of 10 on the CVSS scale, the vulnerability is especially dangerous because of its ability to be exploited remotely without user interaction and with low privileges.

The pipelines in GitLab are automated workflows, such as tests or deployments. If an attacker can execute uncontrolled pipelines, they could deploy malicious code in production environments or alter critical tests without authorization, leading to security or service availability failures.

GitLab has released critical updates that fix this vulnerability in versions 17.3.2, 17.2.5 y 17.1.7. It is recommended thatUsers are advised to immediately apply the available patches.

A temporary mitigation would be to disable pipeline execution on unprotected branches and limit access to critical resources to trusted users until the recommended security patch can be applied. It is also advisable to review user permissions and enforce security rules in CI/CD configurations to prevent exploits during the exposure period.

For more details and access to the updates, please refer to the official official GitLab documentation