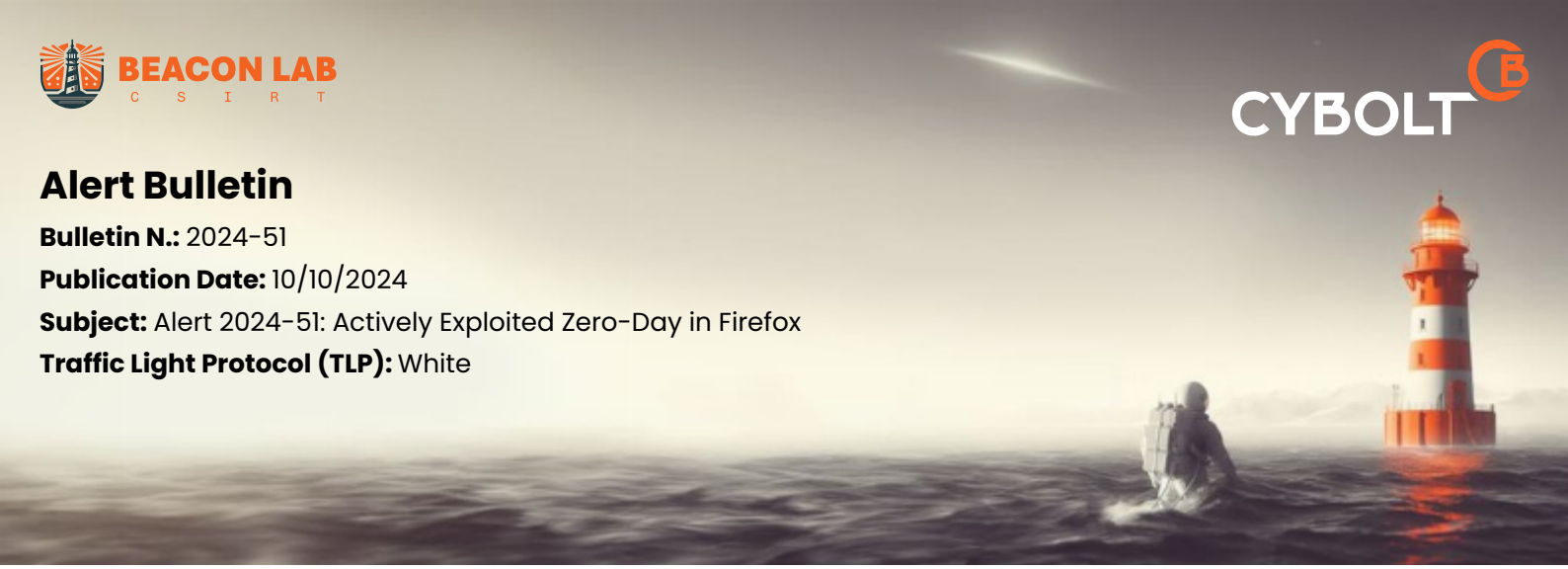

Alert Bulletin

Bulletin N.: 2024-51
Publication Date: 10/10/2024
Subject: Alert 2024-51: Actively Exploited Zero-Day in Firefox
Traffic Light Protocol (TLP): White

Mozilla has released an urgent update for Firefox (version 131.0.2) and Firefox ESR (versions 115.16.1 and 128.3.1) to fix a critical remote code execution vulnerability, CVE-2024-9680. The popular open-source web browser, along with its enterprise and organization versions, has a use-after-free issue in timeline animations, which has been actively exploited in attacks. An attacker can exploit this flaw to execute malicious code in the browser's content process.

Mozilla has released updates to mitigate this vulnerability in the affected versions, and it is recommended that all users update their browsers as soon as possible to prevent potential exploitation of this vulnerability.

You can find more information and details on Mozilla's official website.