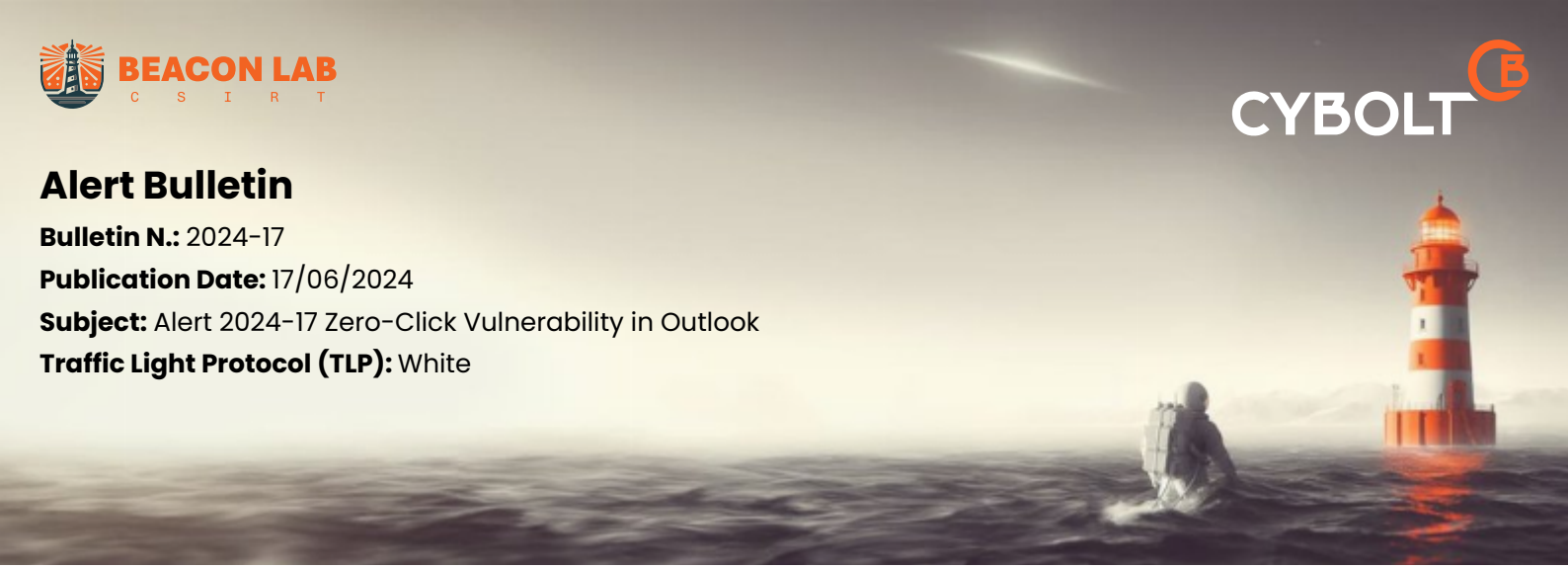

Alert Bulletin

Bulletin N.: 2024-17
Publication Date: 17/06/2024
Subject: Alert 2024-17 Zero-Click Vulnerability in Outlook
Traffic Light Protocol (TLP): White

Affected Product(s):

- MS Outlook clients after version 2016.

Description:

On **June 11, 2024**, Microsoft released a dedicated patch for the vulnerability known as **CVE-2024-30103**, which was discovered a month earlier by **Morphisec researchers**, with a severity score of **8.8**.

This vulnerability was identified on **April 3, 2024**, and reported privately to Microsoft. While details have not yet been disclosed, it is known to be a **zero-click vulnerability**, meaning it does not require user interaction; however, the email containing the exploit must be opened. The vulnerability is particularly critical in environments where the automatic email opening feature is enabled, as it could be exploited without user intervention.

If successfully attacked, malicious DLLs could be injected into the Outlook registry, allowing control over the affected machine.

As of now, there is no public exploit for this vulnerability; however, technical details will be revealed in August, making it highly likely that exploits will soon become available, increasing the likelihood of attacks.

Impact:

A malicious actor who exploits this vulnerability could compromise any mailbox and thereby gain control of the underlying operating system.

Solution:

All users are strongly advised to apply the patch labeled as **“KB5002600”** as soon as possible, as this addresses the vulnerability.