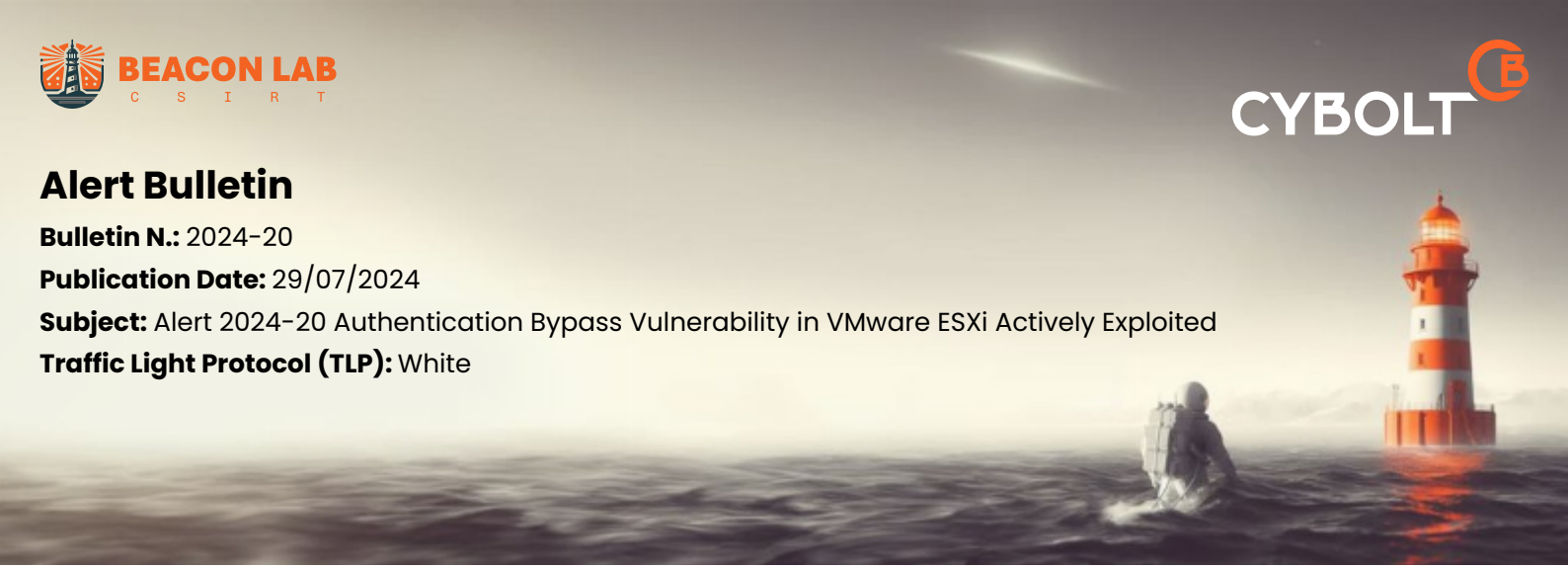

Alert Bulletin

Bulletin N.: 2024-20
Publication Date: 29/07/2024
Subject: Alert 2024-20 Authentication Bypass Vulnerability in VMware ESXi Actively Exploited
Traffic Light Protocol (TLP): White

Affected Product(s):

- VMware ESXi 8.0 and 7.0
- VMware Cloud Foundation 5.x and 4.x

Description:

A medium-severity security flaw, identified as **CVE-2024-37085** with a CVSS score of 5.8, is a **"Active Directory Integration Authentication Bypass"** vulnerability in **VMware ESXi**. This vulnerability was discovered by Microsoft security researchers and fixed with the release of **ESXi 8.0 U3** on June 25.

ESXi is a hardware hypervisor installed directly on physical servers, providing direct access and control over underlying resources. ESXi hypervisors host virtual machines that may include critical servers within a network. The vulnerability affects a domain group whose members have default administrative access to the ESXi hypervisor without proper validation. While a successful attack requires high privileges on the target device and user interaction, it poses significant risks.

Microsoft has reported that multiple ransomware groups are exploiting this vulnerability to escalate to full administrator privileges on domain-joined hypervisors. The vulnerability has been actively exploited by ransomware operators such as **Storm-0506**, **Storm-1175**, **Octo Tempest**, and **Manatee Tempest** in attacks leading to the deployment of ransomware families like **Akira** and **Black Basta**.

Microsoft has identified at least three tactics that attackers may use to exploit CVE-2024-37085, including:

1. Adding the "ESX Admins" group to the domain and adding a user.
2. Renaming any domain group as "ESX Admins" and adding a user to the group or using an existing group member.
3. Updating ESXi hypervisor privileges (assigning admin privileges to other groups without removing them from the "ESX Admins" group).

This vulnerability poses a significant risk to environments using VMware ESXi, especially if administrative protections are weak or not properly enforced.