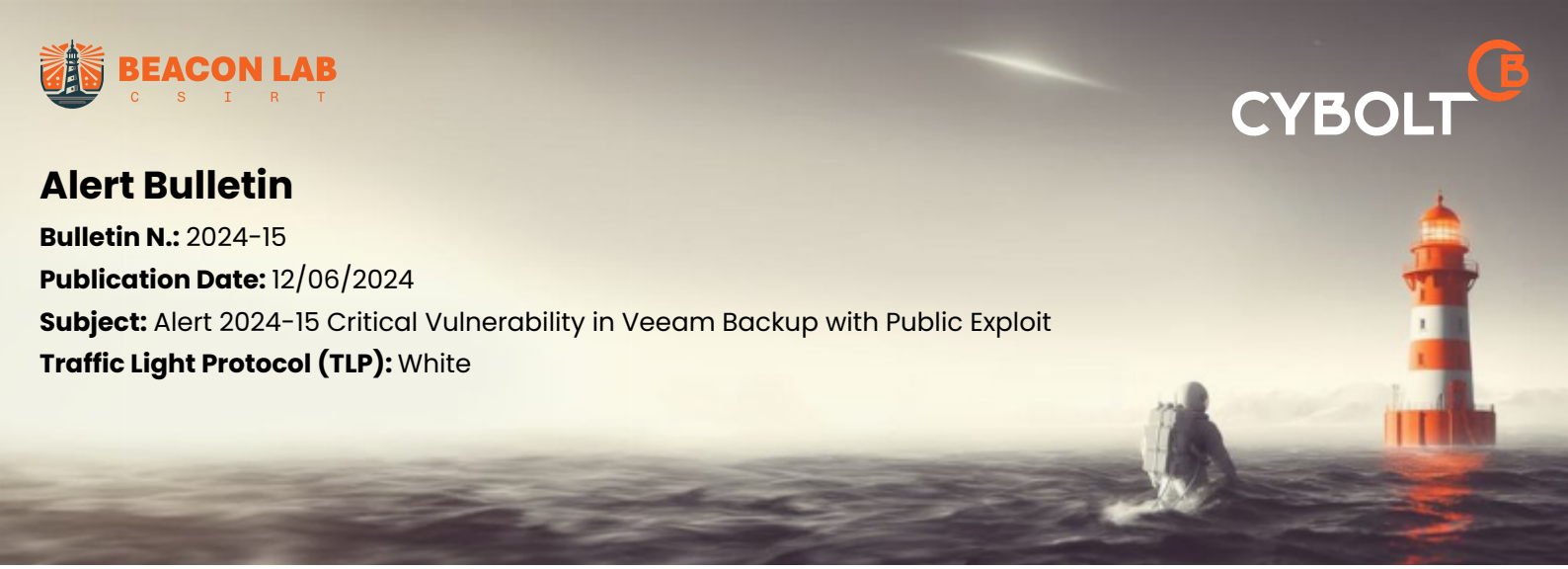

Alert Bulletin

Bulletin N.: 2024-15
Publication Date: 12/06/2024
Subject: Alert 2024-15 Critical Vulnerability in Veeam Backup with Public Exploit
Traffic Light Protocol (TLP): White

Affected Product(s):

- **Veeam Backup Enterprise Manager**

Affected Versions:

- Versions prior to **12.1.2.172**

Description:
On **May 21, 2024**, Veeam announced the discovery of a security flaw in **Veeam Backup Enterprise Manager** software, identified as **CVE-2024-29849**, with a severity score of **9.8** (High).

This vulnerability is an **authentication bypass**, allowing an attacker to manipulate backups within the infrastructure. This is significant because an attacker infiltrating the network could exploit this vulnerability at their convenience to impact backup copies. This technique is commonly used by ransomware groups, who often seek to access and destroy backups before encrypting files.

Recently, a proof of concept exploit for this vulnerability was published, greatly increasing the likelihood of exploitation in enterprise environments, which could lead to substantial production damage if internal backups are also affected.

Impact:

A malicious actor within the network could exploit this vulnerability to partially or completely delete backup copies, making it impossible to revert to a backup for recovery.

Solution:

Update the **Veeam Backup Enterprise Manager** software to version **12.1.2.172** or later.

Additional Information:

- Security Affairs Article

- Veeam Knowledge Base
- Security Boulevard Article
- Summoning Team Blog