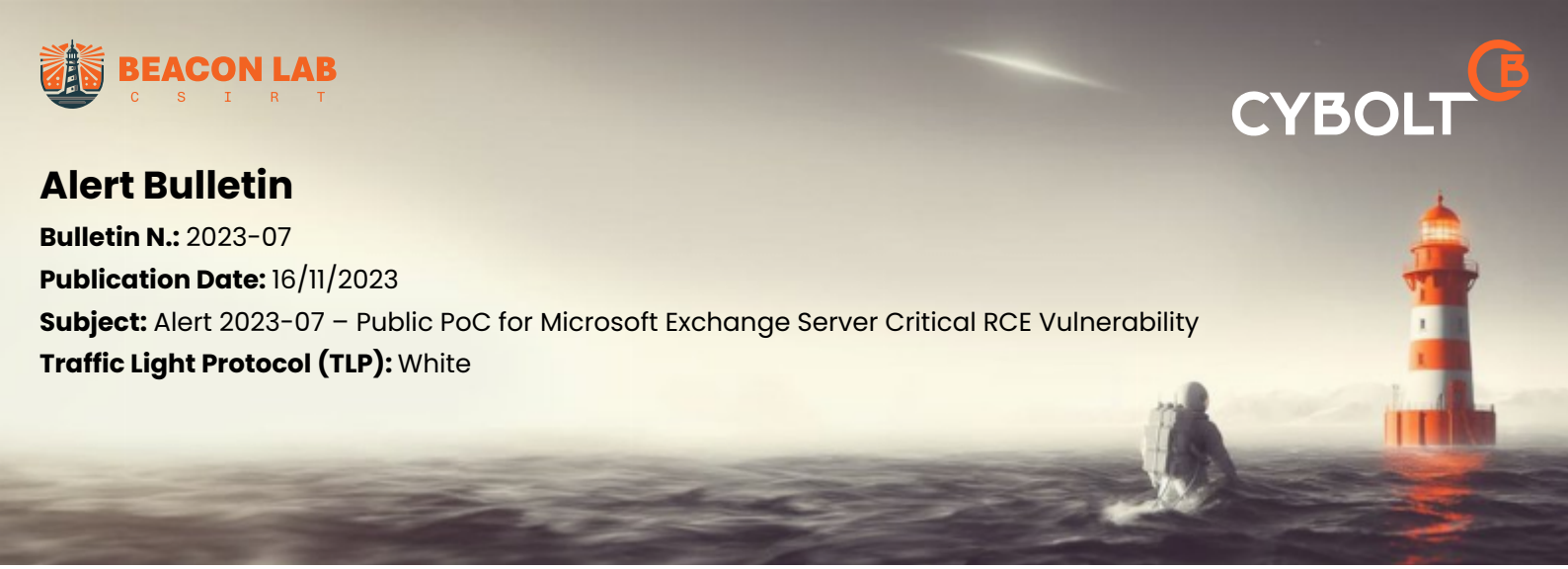

Alert Bulletin

Bulletin N.: 2023-07
Publication Date: 16/11/2023
Subject: Alert 2023-07 – Public PoC for Microsoft Exchange Server Critical RCE Vulnerability
Traffic Light Protocol (TLP): White

A critical vulnerability has been reported affecting Microsoft Exchange Server Mail Server named CVE-2023-36745 rated High with a CVSS score of 8.0, which may allow remote attackers to execute remote code (RCE).

This vulnerability is exploited by leveraging the Microsoft.Exchange.DxStore.Common.DxSerializationUtil.SharedTypeResolver class to bypass the default security restrictions of the .NET Framework. This class can be used to load assemblies from remote locations, which subsequently allows arbitrary code execution on the victim's system.

An attacker could exploit the vulnerability by leveraging the gadget (Type 4) UnitySerializationHolder by deserializing untrusted data. Exploitation of this vulnerability requires the attacker to gain access to the LAN and obtain credentials for a valid Exchange user.

A Proof of Concept (PoC) exploit for Microsoft Exchange Server vulnerability CVE-2023-36745 has been published, it is recommended to take immediate corrective action.