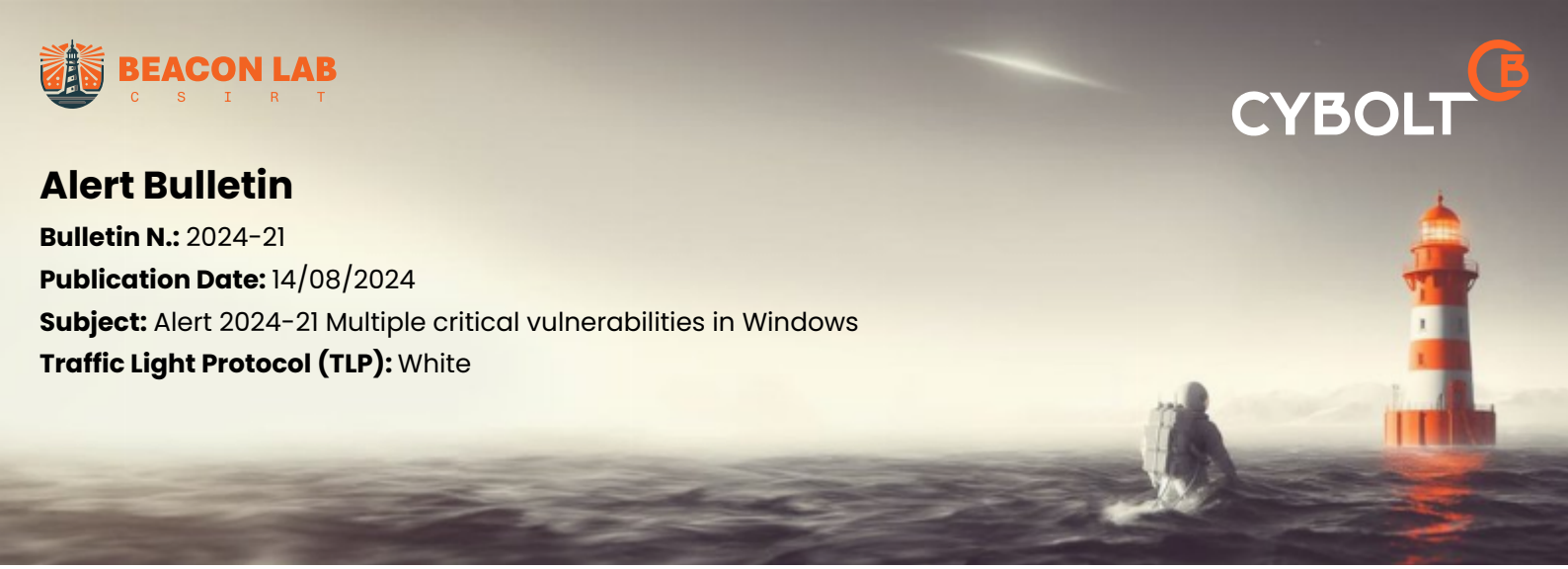

Alert Bulletin

Bulletin N.: 2024-21
Publication Date: 14/08/2024
Subject: Alert 2024-21 Multiple critical vulnerabilities in Windows
Traffic Light Protocol (TLP): White

Product(s) affected:

- Multiples products Microsoft products

Description

his month, Microsoft released a patch that fixes 90 new vulnerabilities affecting various products, including Windows and its components, Office and Office Components, .NET and Visual Studio, Azure, Co-Pilot, Microsoft Dynamics, Teams and Secure Boot.

Of the published updates, seven are classified as critical, 79 as important and one as moderate in severity, some of them with active exploitation.

You can consult the complete list of CVEs published by Microsoft at the following link: https://msrc.microsoft.com/update-guide/releaseNote/2024-Aug.).

Some of the most relevant vulnerabilities are highlighted below:

- **CVE-2024-38063**Remote code execution on Windows TCP/IP.

This is a critical RCE vulnerability with a CVSSv3 score of 9.8, classified as “Most Likely Exploit”. An attacker could exploit it remotely by sending specially crafted IPv6 packets to a host.

- **CVE-2024-38140**Remote code execution in Windows Reliable Multicast Transport Driver (RMCAST).

Another critical RCE vulnerability, with a CVSSv3 score of 9.8. An unauthenticated attacker could exploit it by sending crafted packets to a Windows Pragmatic General Multicast (PGM) socket, without requiring user interaction.