Alert Bulletin

Bulletin N.: 2024-23
Publication Date: 06/09/2024
Subject: Alert 2024-23 Public PoC Affecting a Critical Vulnerability in Windows
Traffic Light Protocol (TLP): White

On **August 13, 2024**, a critical vulnerability identified as **CVE-2024-38063** was disclosed, with a severity score of **9.8**. This remote code execution (RCE) vulnerability affects the **TCP/IP stack in Windows**, specifically targeting the **IPv6 protocol**.

This **Zero-Click** flaw (requiring no user or victim interaction) allows attackers to remotely execute arbitrary code through specially crafted **IPv6 packets**, potentially leading to a complete system compromise. It impacts **Windows 10**, **Windows 11**, and **Windows Server** systems. Microsoft has released patches to mitigate this vulnerability, and it is essential to apply these updates promptly to protect against exploitation.

A **Proof of Concept (PoC)** for this vulnerability has been published. The researcher notes that the current version of the PoC triggers a **denial of service (DoS)** rather than full remote code execution.

Despite this, the existence of the PoC serves as a clear reminder of the potential for further exploitation, particularly as attackers refine their techniques.