Alert Bulletin

Bulletin N.: 2023-06
Publication Date: 16/11/2023
Subject: Alert 2023-06 – Critical Vulnerabilities Reported in VMware Products
Traffic Light Protocol (TLP): White

A critical vulnerability affecting VMware vCenter Server products has **been reported** that could result in remote code execution (RCE) on affected systems.

The issue, identified as **CVE-2023-34048** with score **9.8**, has been described as an out-of-bounds write vulnerability in the implementation of the **DCE/RPC protocol**. "A malicious actor with access to the vCenter Server network can trigger an out-of-bounds write that could lead to remote code execution," VMware **said** in a published advisory.

In addition, vCenter Server contains a partial information disclosure vulnerability. VMware has assessed the severity of this issue in the moderate severity range identified as **CVE-2023-34056** with a score of **4.3.**

Several vulnerabilities have also been **reported** in VMware Aria Operations for Logs. Fortunately there are also updates already available to remediate this vulnerability.

VMware Aria Operations for Logs contains two vulnerabilities: **CVE-2023-34051** authentication bypass and **CVE-2023-34052** bad deserialization. In addition, VMware has assessed the severity of both in the major severity range with a score of **8.1** each.