Alert Bulletin

Bulletin N.: 2024-36
Publication Date: 18/09/2024
Subject: Alert 2024-36 Critical Vulnerability in VMware CVE-2024-38812
Traffic Light Protocol (TLP): White

Affected Product(s):

- VMware vCenter Server
- VMware Cloud Foundation

Description:

A critical vulnerability has been identified in VMware's vCenter Server platform, known as CVE-2024-38812, reported by TZL researchers during the Matrix Cup 2024 hacking contest in China. This vulnerability, with a CVSS severity score of 9.8, stems from a stack overflow in the DCE/RPC protocol implementation in vCenter Server, allowing remote code execution via specially crafted packets. Attackers with network access could fully compromise the vCenter environment, severely impacting the organization's virtualized infrastructure.

Additionally, CVE-2024-38813, a privilege escalation vulnerability to root, has also been reported. Both vulnerabilities pose severe risks to enterprise security, enabling both remote code execution and privilege escalation.

It is strongly recommended to apply the security updates provided by VMware immediately to mitigate these risks and prevent system compromises.

These issues require urgent attention to avoid security incidents that could compromise critical environments.