# Critical Vulnerability Found in VMware vCenter Server – CVE-2024-38812 and CVE-2024-38813

## Overview

On September 17, 2024, Broadcom released patches for VMware vCenter Server to address two significant vulnerabilities, CVE-2024-38812 and CVE-2024-38813. These vulnerabilities were discovered during the 2024 Matrix Cup hacking competition and could lead to remote code execution (RCE) and privilege escalation. Currently, the vulnerabilities are not being exploited.

**CVE-2024-38812 (CVSS 9.8)**

- This vulnerability is a heap-overflow flaw within the DCE/RPC protocol in VMware vCenter Server. It can be exploited remotely by an attacker sending a specially crafted network packet that could result in RCE.

**CVE-2024-38813 (CVSS 7.5)**

- This vulnerability allows authenticated attackers to escalate privileges to root, which is a risk within affected environments.

Affected products include:

- VMware vCenter Server versions 8.0 and 7.0
- VMware Cloud Foundation versions 5.x and 4.x (as it includes vCenter)

Although CVE-2024-38812 and CVE-2024-38813 have not been exploited, Aspire strongly recommends patching as soon as possible.

## Aspire Protects

- **Apply Patches**: Admins should update VMware vCenter Server to the fixed versions (8.0 U3b, 7.0 U3s) as soon as possible. For patch guidance and release notes, please see Broadcom's advisory.
    - VMware Cloud Foundation users should also apply the asynchronous patches provided in the advisory.
- **No Workarounds**: There are no viable workarounds for these vulnerabilities, making patching the only reliable mitigation.
- **Minimal Service Impact**: While updating vCenter Server, management interfaces like the vSphere Client will be briefly unavailable. However, virtual machine and container workloads will remain unaffected during the update process.

**IoCs**

There are no known IoCs for CVE-2024-38812 and CVE-2024-38813 at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

**TTPs to Watch**

- **Tactic: Initial Access (TA0001)**
  - Exploit Public Facing Application (T1190) - Attackers gain initial access by exploiting vulnerabilities in publicly accessible services like VMware vCenter, such as CVE-2024-38812, using specially crafted network packets.
- **Tactic: Privilege Escalation (TA0004)**
  - Exploitation for Privilege Escalation (T1068) - After gaining access, attackers can exploit the privilege escalation vulnerability (CVE-2024-38813) to escalate privileges to root.
- **Tactic: Impact (TA0040)**
  - Data Manipulation (T1565) - Exploiting these vulnerabilities could allow an attacker to manipulate or corrupt data within the vCenter system.
  - Inhibit System Recovery (T1490) - Attackers may tamper with backups or restoration processes to prevent recovery after exploitation.
- **Tactic: Persistence (TA0003)**
  - **Create or Modify System Process (T1543)** - An attacker leveraging these vulnerabilities may create or modify system processes to maintain persistent access to the compromised system.

## Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Security Services**
  - Aspire Managed Security Services provide remote security monitoring and device management – 24 hours a day, 7 days a week. By aggregating and correlating security events from across your IT environment, our remote security monitoring service eliminates "noise" and make sense of what really matters.

- Our managed security portfolio includes:
  - Managed Firewall
  - Managed IDS/IPS
  - Security event monitoring & incident management
  - Managed Cisco ISE (Identity Services Engine)
  - Endpoint Protection

- **Aspire Managed Detection and Response (MDR)**

  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

## Supporting Documentation

VMSA-2024-0019: Questions & Answers - VMware Cloud Foundation (VCF) Blog

Support Content Notification - Support Portal - Broadcom support portal