Multiple Vulnerabilities in VMware Cloud Foundation

Overview

TL;DR

Three high-severity vulnerabilities have been disclosed in VMware Cloud Foundation, affecting versions 4.5.x and 5.x. These flaws include directory traversal, information disclosure, and missing authorization controls.

There are no workarounds. If you're running Cloud Foundation in your environment, you need to apply the latest updates immediately.

VMware has released security updates for Cloud Foundation to address CVE-2025-41229, CVE-2025-41230, and CVE-2025-41231. All three can be exploited by an attacker with network access or local access to the appliance. The vulnerabilities affect environments running Cloud Foundation on both versions 5.x and 4.5.x.

Vulnerability Breakdown

- **CVE-2025-41229** – Directory Traversal (CVSS 8.2)
  A remote attacker with access to port 443 can exploit this flaw to access internal services by navigating outside intended directories. This opens the door to sensitive file access or lateral movement within the system.
- **CVE-2025-41230** – Information Disclosure (CVSS 7.5)
  This vulnerability also requires network access to port 443. It allows an attacker to gain visibility into sensitive information that should not be exposed externally, which could support broader attacks.
- **CVE-2025-41231** – Missing Authorization (CVSS 7.3)
  A local attacker can abuse this flaw to perform unauthorized actions or gain access to limited internal data. This type of issue is often used to escalate privileges or maintain persistence after initial access.

Affected Versions

- VMware Cloud Foundation 5.x – Patch to version 5.2.1.2
- VMware Cloud Foundation 4.5.x – Apply patch documented in KB398008

These are the kinds of vulnerabilities that fly under the radar until someone figures out how to chain them. With no workarounds and all three rated as high severity, Aspire recommends patching immediately.

Aspire Protects

- **Patch –** Patch all affected Cloud Foundation deployments running versions 5.x and 4.5.x. You may find patch guidance in VMware's advisory.
- Restrict external access to management interfaces where possible.
- Monitor for any unexpected access or activity on port 443.
- Conduct a configuration review to verify access controls are correctly enforced.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – CVE-2025-41229 and CVE-2025-41230 may allow remote access through port 443 to internal components.

Credential Access

- Unsecured Credentials [T1552] – The information disclosed through CVE-2025-41230 may support credential harvesting.

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548] – CVE-2025-41231 could allow unauthorized privilege elevation or task execution.

Lateral Movement

- Remote Services [T1021] – Directory traversal may provide paths for movement across connected components.

IoCs

There are no known IoCs associated with the above vulnerabilities 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.

Targeted Industries

VMware Cloud Foundation is widely used in enterprise and government environments with virtualization-heavy infrastructure. These vulnerabilities are especially relevant to:

- Healthcare
- Public Sector

- Retail
- Finance
- Manufacturing

Aspire 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 cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Support Content Notification - Support Portal - Broadcom support portal

NVD - CVE-2025-41229

NVD - CVE-2025-41230

NVD - CVE-2025-41231