Exploited VMware vCenter Server Flaws Threaten Virtualized Environments

TL;DR

VMware patched three critical vCenter Server vulnerabilities (CVE-2024-37079, CVE-2024-37080, and CVE-2024-37081) that allow remote code execution and local privilege escalation.

One of them, CVE-2024-37079, has been exploited in the wild. If vCenter is exposed or reachable on the network, patch immediately.

Overview

VMware patched three vulnerabilities (CVE-2024-37079, CVE-2024-37080, and CVE-2024-37081) in vCenter Server that affect core management infrastructure used across virtualized environments. The issues include two heap-overflow flaws in the DCERPC service that can lead to remote code execution, along with a local privilege escalation weakness tied to sudo configuration.

Affected Products

- VMware vCenter Server 7.x
- VMware vCenter Server 8.x
- VMware Cloud Foundation (vCenter Server deployments)

Broadcom confirmed CVE-2024-37079 has been exploited, which raises the risk for environments that have not been patched. Because vCenter controls core virtualization functions, a successful compromise gives an attacker deep access into the environment.

CVE-2024-37079 and CVE-2024-37080 – Heap Overflow Leading to Remote Code Execution (CVSS 9.8)

- These vulnerabilities stem from how vCenter Server handles DCERPC network traffic. A remote attacker with network access to the vCenter Server service can send specially crafted packets that corrupt memory and allow arbitrary code execution.
- No authentication is required. Broadcom stated that CVE-2024-37079 has already been abused in real attacks, increasing concern for exposed or internally reachable systems.

CVE-2024-37081 – Local Privilege Escalation via Sudo Misconfiguration (CVSS 7.8)

- This issue allows a local, non-administrative user to escalate privileges to root on the vCenter Server Appliance.
- While it requires authenticated access, it becomes especially dangerous when chained with another vulnerability or post-compromise access.

Successful exploitation of these remote code execution flaws could allow attackers to gain control over hosts, workloads, and connected environments. Due to the severity of the vulnerabilities and confirmed exploitation, Aspire recommends patching immediately.

Aspire Protects

- **Patch** – Patching is the only effective mitigation. Please patch as soon as possible. See Broadcom's advisory for more information.
  - vCenter Server 8.0 – Upgrade to 8.0 U2d or 8.0 U1e
  - vCenter Server 7.0 – Upgrade to 7.0 U3r
  - VMware Cloud Foundation 4.x / 5.x – Apply KB88287
- Defensive Monitoring
  - vCenter Server logs for unexpected DCERPC-related activity
  - Abnormal processes or command execution on the vCenter Server Appliance
  - Unapproved sudo usage or privilege escalation events
  - Configuration changes or service modifications on vCenter

TTPs

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker exploited heap-overflow vulnerabilities in the vCenter Server DCERPC service by sending crafted network packets to a reachable management interface, resulting in remote code execution without authentication (CVE-2024-37079, CVE-2024-37080).

Execution

- Command and Scripting Interpreter [T1059] – The attacker executed arbitrary operating system commands on the vCenter Server Appliance following successful exploitation of the DCERPC service.

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548] – The attacker abused misconfigured sudo permissions to escalate privileges from a non-administrative local account to root on the vCenter Server Appliance (CVE-2024-37081).

IoCs

There are no known IoCs 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

Organizations running VMware vCenter Server or VMware Cloud Foundation are at risk, particularly those relying on centralized virtualization management for daily operations.

- Government
- Education
- Energy
- Healthcare
- Retail
- Finance
- Technology
- Legal
- Manufacturing

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 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