Critical VMware Vulnerabilities Allow Authentication Bypass, Remote Code Execution and VM Escape

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

Broadcom patched five vulnerabilities affecting VMware vCenter, ESX, Workstation and Fusion.

The most serious flaws could allow an unauthenticated attacker to bypass vCenter authentication, execute arbitrary code or escape from a compromised virtual machine and execute code on the ESX host.

Overview

There are five vulnerabilities, including three critical flaws, affecting VMware vCenter, ESX, Workstation and Fusion. VMware vCenter provides centralized management for virtual machines and ESX hosts, while ESX runs and manages virtualized workloads.

The vulnerabilities include:

- **CVE-2026-59309** (CVSS 9.8) - An authentication-bypass vulnerability in the VMware Directory Service. An unauthenticated attacker with network access to vCenter may exploit the vulnerability to bypass authentication and gain unauthorized access to the system.
- **CVE-2026-59310** (CVSS 9.8) - A directory-traversal vulnerability in the vCenter Syslog server. An unauthenticated attacker with network access to vCenter may exploit the vulnerability to execute arbitrary code.
- **CVE-2026-47876** (CVSS 9.3) - An out-of-bounds write vulnerability in the VMXNET3 virtual network adapter. An attacker with local administrative privileges on a virtual machine using VMXNET3 may exploit the vulnerability to escape the virtual machine and execute code on the ESX host. Virtual machines using other virtual network adapters are not affected. The vulnerability was successfully demonstrated during Pwn2Own Berlin 2026.
- **CVE-2026-41703** (CVSS 7.6) - An out-of-bounds read vulnerability affecting VMware ESX, Workstation and Fusion. An attacker with VM deployment privileges may exploit the vulnerability to disclose information or cause a denial-of-service condition on the host process. The impact on Workstation and Fusion is limited to information disclosure.

- **CVE-2026-41709** (CVSS 2.7) - An insufficient-logging vulnerability in VMware ESX. A malicious administrator may exploit the vulnerability to perform certain operations without those actions being logged.

Affected Products

- VMware ESX
- VMware vCenter
- VMware Workstation
- VMware Fusion
- VMware Cloud Foundation
- VMware vSphere Foundation
- VMware Telco Cloud Platform
- VMware Telco Cloud Infrastructure

Broadcom reported no available workarounds. There is currently no evidence that the vulnerabilities are being exploited in attacks. However, CVE-2026-59309 and CVE-2026-59310 require only network access to vCenter and no authentication, making exposed or broadly accessible management interfaces vulnerable.

Aspire Protects

- Apply the fixed versions listed in Broadcom security advisory.
- Restrict vCenter access to authorized management networks and administrators.
- Block direct internet access to vCenter and ESX management interfaces.
- Review vCenter and ESX administrative accounts for unauthorized additions or changes.
- Review vCenter, ESX and network logs for unexpected authentication activity, configuration changes or access from unfamiliar systems.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – An attacker may exploit CVE-2026-59309 or CVE-2026-59310 through a network-accessible vCenter server to bypass authentication or execute arbitrary code.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – An attacker with administrative access to a virtual machine using VMXNET3 may exploit CVE-2026-47876 to escape the virtual machine and execute code on the ESX host.

Impact

- Endpoint Denial of Service [T1499] – An attacker with VM deployment privileges may exploit CVE-2026-41703 to cause a denial-of-service condition affecting an ESX host process.

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

The vulnerabilities may affect organizations across all sectors that use VMware products to manage virtualized servers and workloads, particularly:

- Government
- Defense
- Technology
- Healthcare
- Telecommunications
- Finance
- Education
- Retail

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