

Alert Bulletin

Bulletin N.: 79

Publication Date: 29/07/2026

Subject: Alert 2026-79 Critical Vulnerabilities in VMware vCenter, ESXi, Workstation, and Fusion

Traffic Light Protocol (TLP): White

Affected product(s):

- **VMware vCenter Server**

9.1.x (fixed in 9.1.0.0300)

9.0.x (fixed in 9.0.2.0100)

8.0.x (fixed in 8.0)

7.0.x (affected; fixes will only be available for customers with an Extended Support contract).

- **VMware ESXi**

9.1.x (fixed in 9.1.0.0200)

9.0.x (fixed in 9.0.2.0100)

8.0.x (fixed in 8.0)

7.0.x (affected; Broadcom indicates that patches may be obtained through Extended Support).

- **VMware Workstation Pro**

25H2 (fixed by upgrading to 26H1).

- **VMware Fusion**

25H2 (fixed by upgrading to 26H1).

Description

Broadcom, through the VMware Security Response Center (vSRC), published advisory [**VMSA-2026-0006**](#), which fixes five security vulnerabilities affecting VMware vCenter Server, ESXi, Workstation, and Fusion. Three

of them were classified as critical (CVSS up to 9.8) because they allow compromising essential components of the virtualization infrastructure, while the remaining two have a significant impact on the confidentiality and traceability of security events. At the time of publication, there was no public evidence of active exploitation, although Broadcom recommends applying the updates as a priority. The most critical vulnerabilities are described below:

CVE-2026-59309 (CVSS 9.8) – Authentication Bypass in VMware vCenter

A flaw in VMware Directory Service (vmdir) allows an attacker with network access to bypass the vCenter Server authentication mechanism and obtain unauthorized access to the system without the need for valid credentials. Because vCenter is the central management point for VMware infrastructures, exploitation of this vulnerability could completely compromise the virtualization platform.

CVE-2026-59310 (CVSS 9.8) – Remote Code Execution via Directory Traversal

This vulnerability resides in the VMware vCenter Syslog server and combines a Directory Traversal condition that can lead to remote code execution (RCE). An unauthenticated attacker with network access could execute arbitrary code on the vCenter server, gaining control of the system and facilitating lateral movement within the virtualized environment.

CVE-2026-47876 (CVSS 9.3) – Virtual Machine Escape in ESXi

It affects the VMXNET3 virtual network adapter through an Out-of-Bounds Write vulnerability. An attacker who gains administrative privileges within a virtual machine could escape the virtual environment and execute code directly on the ESXi host. This vulnerability only affects virtual machines that use the VMXNET3 adapter, one of the most widely used in VMware environments due to its high performance.

Solution:

Broadcom published security updates for all affected platforms through advisory [VMSA-2026-0006](#), where the official patches can be found. The main recommendation is to immediately update vCenter Server, ESXi, VMware Workstation, and VMware Fusion to the fixed versions indicated in the vendor's response matrix.

In the case of CVE-2026-47876, it is recommended to identify the virtual machines that use the VMXNET3 adapter, as only they are susceptible to this vulnerability. However, Broadcom clarifies that it is not necessary to update VMware Tools, since the fix is in the hypervisor and not in the guest operating system.

It is also recommended to restrict administrative access to vCenter, properly segment management networks, limit the exposure of management services only to trusted networks, and monitor any anomalous access attempts while the updates are being implemented.

Additional information:

- <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017?ref=darkwebinformers.com>
- <https://www.broadcom.com/support/vmware-services/security-response>

- <https://darkwebinformers.com/broadcom-patches-critical-vmware-flaws-enabling-vcenter-authentication-bypass-and-esxi-vm-escape/>