Smarttech
YOUR 24/7 SECURITY PARTNER

# Multiple Vulnerabilities in VMware Products – 29th July 2026

| | |
|---|---|
| **Document ID** | SMA-Threat Report |
| **Document status** | ISSUED |
| **Issue Number** | 126 |
| **Authors** | Alex Ciuta < alexandru.ciuta@smarttech247.com > |
| **Verified by** | Alin Curcan < alin.curcan@smarttech247.com > |
| **Last modified** | 2026-07-29 |
| **Issue Date** | 2026-07-29 |

**Threat Reports** are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

## Overview:

Multiple vulnerabilities in VMware ESX, vCenter, Workstation, and Fusion were privately reported to Broadcom. Updates are available to remediate these vulnerabilities in affected Broadcom products.

## Risk

**Government**:

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses**:

- Large and medium business entities: **High**
- Small business entities: **High**

## Technical summary

More details related to these vulnerabilities are as follows:

| CVE ID | Description | Known Attack Vectors |
|---|---|---|
| **CVE-2026-59309**<br>**CVSS Base Score: 9.8** | VMware vCenter contains an authentication bypass vulnerability in the VMware Directory Service. | A malicious actor with network access to vCenter may exploit this issue to bypass authentication and gain unauthorized access to the system. |
| **CVE-2026-59310**<br>**CVSS Base Score: 9.8** | VMware vCenter contains a directory traversal vulnerability in the Syslog server. | A malicious actor with network access to vCenter may exploit this issue to execute arbitrary code. |
| **CVE-2026-47876**<br>**CVSS Base Score: 9.3** | VMware ESX contains an out-of-bounds write vulnerability in the VMXNET3 virtual network adapter. | A malicious actor with local administrative privileges on a virtual machine with VMXNET3 virtual network adapter may exploit this issue to execute code on the host. Non VMXNET3 virtual adapters are not affected by this issue. |
| **CVE-2026-41703**<br>**CVSS Base Score: 7.6** | VMware ESX, Workstation, and Fusion contain an out-of-bounds read vulnerability. | A malicious actor with VM deployment privileges could trigger an out-of-bounds read, potentially leading to information disclosure or more likely a Denial-of-Service (DoS) condition of the host |

| | | |
|---|---|---|
| | | process. On Workstation and Fusion, the impact of this vulnerability is restricted to information disclosure. |
| **CVE-2026-41709**<br>**CVSS Base Score: 7.6** | VMware ESX contains an insufficient logging vulnerability. | A malicious administrator could exploit this issue to perform certain operations without them 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

## Response Matrix

| Product | Component | Version | Running On | CVE | CVSSv3 | Severity | Fixed Version |
|---|---|---|---|---|---|---|---|
| VMware Cloud Foundation, VMware vSphere Foundation | vCenter | 9.1.x.x | Any | CVE-2026-59309, CVE-2026-59310 | 9.8 | Critical | 9.1.0.0300 |
| VMware Cloud Foundation,<br><br>VMware vSphere Foundation | vCenter | 9.0.x.x | Any | CVE-2026-59309, CVE-2026-59310 | 9.8 | Critical | 9.0.2.0100 |
| VMware vCenter | N/A | 8.0 | Any | CVE-2026-59309, CVE-2026-59310 | 9.8 | Critical | 8.0 U3k |
| VMware Cloud Foundation | vCenter | 5.x | Any | CVE-2026-59309, CVE-2026-59310 | 9.8 | Critical | Async patch to 8.0 U3k |
| VMware Telco Cloud Platform | vCenter | 3.0, 4.x, 5.0.x, 5.1.x | Any | CVE-2026-59309, CVE-2026-59310 | 9.8 | Critical | KB449886 |
| VMware Telco Cloud Infrastructure | vCenter | 3.0 | Any | CVE-2026-59309, CVE-2026-59310 | 9.8 | Critical | KB449886 |
| VMware Cloud Foundation, VMware vSphere Foundation | ESX | 9.1.x.x | Any | CVE-2026-47876 | 9.3 | Critical | ESXi-9.1.0.0200-25557999 |
| VMware Cloud Foundation, | ESX | 9.0.x.x | Any | CVE-2026-47876 | 9.3 | Critical | ESXi-9.0.2.0100-25595025 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| VMware vSphere Foundation | | | | | | | |
| VMware ESX | N/A | 8.0 | Any | CVE-2026-47876 | 9.3 | Critical | ESXi80U3k-25595708 |
| VMware Cloud Foundation | ESX | 5.x | Any | CVE-2026-47876 | 9.3 | Critical | Async Patching Guide: KB88287 |
| VMware Telco Cloud Platform | ESX | 5.0.x, 5.1.x | Any | CVE-2026-47876 | 9.3 | Critical | KB449886 |
| VMware Cloud Foundation, VMware vSphere Foundation | ESX | 9.1.x.x | Any | CVE-2026-41703 | 7.6 | Important | ESXi-9.1.0.0-25370933 |
| VMware Cloud Foundation, VMware vSphere Foundation | ESX | 9.0.x.x | Any | CVE-2026-41703 | 7.6 | Important | ESXi-9.0.2.0100-25595025 |
| VMware ESX | N/A | 8.0 | Any | CVE-2026-41703 | 7.6 | Important | ESXi80U3i-25205845 |
| VMware Workstation | N/A | 25H2 | Any | CVE-2026-41703 | 2.7 | Low | 26H1 |
| VMware Fusion | N/A | 25H2 | Any | CVE-2026-41703 | 2.7 | Low | 26H1 |
| VMware Cloud Foundation | ESX | 5.x | Any | CVE-2026-41703 | 7.6 | Important | 5.2.3 |
| VMware Telco Cloud Platform | ESX | 5.0.x, 5.1.x | Any | CVE-2026-41703 | 7.6 | Important | KB449886 |
| VMware Cloud Foundation, VMware vSphere Foundation | ESX | 9.1.x.x | Any | CVE-2026-41709 | 2.7 | Low | ESXi-9.1.0.0-25370933 |
| VMware Cloud Foundation, VMware vSphere Foundation | ESX | 9.0.x.x | Any | CVE-2026-41709 | 2.7 | Low | ESXi-9.0.2.0100-25595025 |
| VMware ESX | N/A | 8.0 | Any | CVE-2026-41709 | 2.7 | Low | ESXi80U3j-25429389 |
| VMware Cloud Foundation | ESX | 5.x | Any | CVE-2026-41709 | 2.7 | Low | 5.2.4 |
| VMware Telco Cloud Platform | ESX | 5.0.x, 5.1.x | Any | CVE-2026-41709 | 2.7 | Low | KB449886 |

## Recommendations

**Smarttech247 team** recommend the following actions be taken:

- **Upgrade** VMware to the fixed version.
- **Upgrade** software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- **Use** the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.

- **Apply** the Principle of Least Privilege to all systems and services.
- **Apply** advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- **Ensure** that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

## References

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

## CVE

CVE-2026-59309,
CVE-2026-59310,
CVE-2026-47876,
CVE-2026-41703,
CVE-2026-41709

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com