

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| Close-up of a silver and brown spoon  AI-generated content may be incorrect. |  | |  |  |  |  | | --- | --- | --- | --- | | As the **Attack Surface** expands, and with the rise of more sophisticated threat actors, vulnerability management has shifted from a reactive stance to a proactive and predictive approach. This transformation calls for the embrace of risk-based methodologies, utilization of advanced threat intelligence, and alignment with the broader security architecture. Contemporary vulnerability management must take into account an organization's distinct threat environment and customize remediation strategies accordingly.  This is where our proactive **Advanced Vulnerability Management (AVM)** services come to play and help you to build a robust Vulnerability Management System which is based on a Risk-Based Approach, Asset Value, Severity of Vulnerabilities, and Threat Actors. | | | | |  |  |  |  | |  |
|  | | | |

|  |
| --- |
| [VMware ESXi, vCenter Server, Workstation, and Fusion updates address multiple vulnerabilities](https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25717) |

**Vulnerability Detail & Resolution:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **VMSA-2025-0010: VMware ESXi, vCenter Server, Workstation, and Fusion updates address multiple vulnerabilities (CVE-2025-41225, CVE-2025-41226, CVE-2025-41227, CVE-2025-41228)**   |  |  |  |  |  | | --- | --- | --- | --- | --- | | CVSS Score Rating | | | | | | Severity | Low | Medium | High | Critical | | CVSS Score | 0.1-3.9 | 4.0-6.9 | 7.0-8.9  ✓ | 9.0-10.0 | |
| * VMware vCenter Server authenticated command-execution vulnerability (CVE-2025-41225):   **Description**: The vCenter Server contains an authenticated command-execution vulnerability. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.8.  CVE-2025-41225 is an authenticated command-execution vulnerability in VMware vCenter Server that allows a privileged attacker to execute arbitrary commands. This type of CVE generally impacts system integrity and can lead to full administrative compromise if exploited in environments with inadequate privilege separation.  **Security Impact**: An attacker with sufficient permission could leverage this flaw to execute unauthorized commands, potentially leading to data breaches, lateral movement, or service disruption, undermining both confidentiality and system control.  **Known Attack Vectors**: A malicious actor with privileges to create or modify alarms and run script action may exploit this issue to run arbitrary commands on the vCenter Server.   * Guest Operations Denial-of-Service Vulnerability (CVE-2025-41226)   **Description**: VMware ESXi contains a denial-of-service vulnerability that occurs when performing a guest operation. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 6.8.  CVE-2025-41226 is a denial-of-service (DoS) vulnerability in VMware ESXi triggered during guest operations, allowing an authenticated user to disrupt virtual machine availability. In general, such CVEs impact system availability and can halt workloads or degrade service reliability.  **Security Impact**: An attacker with guest operation privileges could exploit this vulnerability to crash or freeze guest VMs, leading to service outages or performance degradation. While it doesn’t allow code execution or data access, it poses a risk to system uptime and operational continuity.  **Known Attack Vectors**: A malicious actor with guest operation privileges on a VM, who is already authenticated through vCenter Server or ESXi may trigger this issue to create a denial-of-service condition of guest VMs with VMware Tools running and guest operations enabled.   * Denial-of-Service Vulnerability (CVE-2025-41227)   **Description:** VMware ESXi, Workstation, and Fusion contain a denial-of-service vulnerability due to certain guest options. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 5.5.  CVE-2025-41227 is a denial-of-service vulnerability that affects VMware ESXi, Workstation, and Fusion, allowing a low-privileged guest user to exhaust host process memory. Such vulnerabilities typically impact system availability by crashing or degrading virtualized environments.  **Security Impact**: An attacker within a guest OS could trigger resource exhaustion, causing host-side denial-of-service. While it doesn’t allow system compromise, it can disrupt hosted workloads and affect service reliability.  **Known Attack Vectors**: A malicious actor with non-administrative privileges within a guest operating system may be able to exploit this issue by exhausting memory of the host process leading to a denial-of-service condition.   * VMware ESXi and vCenter Server Reflected Cross Site Scripting (XSS) Vulnerability (CVE-2025-41228)   **Description**: VMware ESXi and vCenter Server contain a reflected cross-site scripting vulnerability due to improper input validation. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 4.3.  CVE-2025-41228 is a reflected cross-site scripting (XSS) vulnerability in VMware ESXi and vCenter Server, stemming from improper input validation. In general, XSS flaws can enable session hijacking, redirection, or manipulation of browser-side content.  **Security Impact**: An attacker could craft a malicious link targeting the login interface to steal session data or trick users into accessing malicious content. While it doesn’t impact backend systems directly, it compromises user trust and interface integrity.  **Known Attack Vectors**: A malicious actor with network access to the login page of certain ESXi host or vCenter Server URL paths may exploit this issue to steal cookies or redirect to malicious websites.  **Products Affected:**   * VMware ESXi * VMware vCenter Server * VMware Workstation Pro * VMware Fusion * VMware Cloud Foundation * VMware Telco Cloud Platform * VMware Telco Cloud Infrastructure   **Publication date:** 20 May 2025 **CVSSv3 Score Range:** 4.3 – 8.8 |