

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| 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、および Fusion のアップデートは、複数の脆弱性に対応しております。 |

**脆弱性の詳細および対応策：**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 における認証済みコマンド実行の脆弱性（CVE-2025-41225）：   **説明: vCenter Server には、認証済みコマンド実行の脆弱性が存在します。VMware は本件の深刻度を「Important」範囲と評価しており、最大 CVSSv3 基本値は 8.8 です。**  CVE-2025-41225は、VMware vCenter Serverに存在する認証済みコマンド実行の脆弱性であり、特権を有する攻撃者が任意のコマンドを実行できる可能性がございます。この種のCVEは一般的にシステムの完全性に影響を及ぼし、権限分離が不十分な環境において悪用された場合、管理者権限の完全な侵害につながる恐れがございます。  **セキュリティへの影響：十分な権限を持つ攻撃者が本脆弱性を悪用することで、不正なコマンドを実行される可能性があります。その結果、情報漏洩、水平移動、またはサービスの中断が発生し、機密性およびシステム制御が損なわれる恐れがあります。**  **既知の攻撃ベクター：アラームの作成または変更、およびスクリプトアクションの実行権限を有する悪意のある攻撃者が、本脆弱性を悪用し、vCenter Server上で任意のコマンドを実行する可能性があります。**   * ゲストオペレーションにおけるサービス拒否の脆弱性（CVE-2025-41226）   **説明: VMware ESXi には、ゲスト操作を実行する際に発生するサービス拒否の脆弱性が存在します。VMware は本件の深刻度を「中程度」と評価しており、最大 CVSSv3 基本値は 6.8 です。**  CVE-2025-41226は、VMware ESXiにおけるサービス拒否（DoS）脆弱性であり、ゲストオペレーション中に発生します。認証済みユーザーによって仮想マシンの可用性が妨害される可能性があります。一般的に、この種のCVEはシステムの可用性に影響を及ぼし、ワークロードの停止やサービスの信頼性低下を引き起こす恐れがあります。  **セキュリティ影響：ゲストオペレーション権限を有する攻撃者が本脆弱性を悪用することにより、ゲストVMをクラッシュまたはフリーズさせ、サービス停止やパフォーマンス低下を引き起こす可能性がございます。本脆弱性はコード実行やデータアクセスを許可するものではございませんが、システムの稼働時間および業務継続性に対するリスクとなります。**  **既知の攻撃ベクトル：VM上でゲスト操作権限を有し、かつvCenter ServerまたはESXiを通じて既に認証されている悪意のある攻撃者が、本脆弱性を悪用することで、VMware Toolsが稼働しゲスト操作が有効化されているゲストVMに対し、サービス拒否（DoS）状態を引き起こす可能性がございます。**   * サービス拒否の脆弱性（CVE-2025-41227）   **説明: VMware ESXi、Workstation、および Fusion には、特定のゲストオプションに起因するサービス拒否の脆弱性が存在します。VMware は本件の深刻度を「中程度」と評価しており、最大 CVSSv3 基本値は 5.5 です。**  CVE-2025-41227は、VMware ESXi、Workstation、および Fusion に影響を及ぼすサービス拒否の脆弱性です。本脆弱性により、権限の低いゲストユーザーがホストプロセスのメモリを枯渇させることが可能となります。この種の脆弱性は、仮想化環境のクラッシュやパフォーマンス低下を引き起こすことで、システムの可用性に影響を及ぼす傾向があります。  **セキュリティ影響：ゲストOS内の攻撃者がリソース枯渇を引き起こし、ホスト側でサービス拒否（DoS）状態を発生させる可能性があります。本脆弱性はシステムの乗っ取りを許可するものではありませんが、ホスト上で稼働しているワークロードに障害を与え、サービスの信頼性に影響を及ぼす可能性がございます。**  **既知の攻撃ベクター：ゲストオペレーティングシステム内で管理者権限を持たない悪意のある攻撃者が、本脆弱性を悪用し、ホストプロセスのメモリを枯渇させることにより、サービス拒否（DoS）状態を引き起こす可能性がございます。**   * VMware ESXi および vCenter Server におけるリフレクテッド型クロスサイトスクリプティング（XSS）脆弱性（CVE-2025-41228）   **説明: VMware ESXi および vCenter Server には、不適切な入力検証に起因するリフレクテッド型クロスサイトスクリプティングの脆弱性が存在いたします。VMware は本件の深刻度を「中程度」と評価しており、最大 CVSSv3 基本値は 4.3 でございます。**  CVE-2025-41228は、VMware ESXiおよびvCenter Serverにおける入力値の検証不備に起因するリフレクティッド型クロスサイトスクリプティング（XSS）の脆弱性です。一般的に、XSSの脆弱性は、セッションハイジャックやリダイレクト、ブラウザ側コンテンツの改ざんなどを引き起こす可能性がございます。  **セキュリティ影響：攻撃者がログインインターフェースを標的とした悪意のあるリンクを作成し、セッションデータを窃取したり、ユーザーを悪意のあるコンテンツに誘導したりする可能性があります。バックエンドシステムに直接影響を与えるものではありませんが、ユーザーの信頼およびインターフェースの整合性が損なわれる恐れがあります。**  **既知の攻撃ベクター：ネットワーク経由で特定のESXiホストまたはvCenter ServerのログインページURLパスにアクセス可能な悪意のある攻撃者が、本脆弱性を悪用し、クッキーを窃取したり、悪意のあるウェブサイトへリダイレクトさせたりする可能性があります。**  **影響を受ける製品：**   * VMware ESXi * VMware vCenter Server * VMware Workstation Pro * VMware Fusion * VMware Cloud Foundation * VMware Telco Cloud Platform * VMware Telco Cloud Infrastructure   **公開日：2025年5月20日  CVSSv3 スコア範囲：4.3 ～ 8.8** |