|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| 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います。 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **VMware vCenter Server 認証済みコマンド実行の脆弱性（CVE-2025-41225）：**   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 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 | |
| * VMSA-2025-0010: VMware ESXi、vCenter Server、Workstation、および Fusion のアップデートにより、複数の脆弱性（CVE-2025-41225、CVE-2025-41226、CVE-2025-41227、CVE-2025-41228）が修正されました。   **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「重要」と評価しており、CVSSv3 基本値の最大スコアは 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、権限を持つ攻撃者が任意のコマンドを実行できる可能性があります。この種の脆弱性は一般的にシステムの整合性に影響を及ぼし、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あります。  **セキュリティへの影響：十分な権限を持つ攻撃者がこの脆弱性を悪用することで、不正なコマンドを実行し、機密情報の漏洩、ラテラルムーブメント、またはサービス拒否などを引き起こす可能性があります。これにより、機密性およびシステムの制御が損なわれるおそれがあります。**  **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認証済みユーザーによってトリガーされ、仮想マシンの可用性を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与え、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。  **セキュリティへの影響：ゲストオペレーション権限を持つ攻撃者が本脆弱性を悪用することで、ゲスト仮想マシンをクラッシュさせたりフリーズさせたりする可能性があり、サービス停止やパフォーマンス低下を引き起こす恐れがあります。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ありませんが、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。**  **既知の攻撃ベクター：vCenter Server または ESXi を通じて既に認証されている仮想マシン上のゲスト操作権限を持つ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仮想マシンに対してサービス拒否状態を引き起こす可能性があります。**   * 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（Denial of Service）脆弱性です。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与える傾向があります。  **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で、サービス拒否状態を引き起こす可能性があります。**  **セキュリティへの影響：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を発生させる可能性があります。本脆弱性はシステムの侵害を許す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あります。**   * VMware ESXi および vCenter Server における反射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クロスサイトスクリプティングの脆弱性が存在します。VMwareは本件の深刻度を中程度（Moderate）と評価しており、最大CVSSv3基本値は4.3です。**  CVE-2025-41228は、VMware ESXiおよびvCenter Serverに存在するリフレクティッドクロスサイトスクリプティング（クロスサイトスクリプティング、XSS）脆弱性であり、不適切な入力検証に起因しています。一般的に、クロスサイトスクリプティングの脆弱性は、セッションハイジャック、リダイレクト、またはブラウザ側コンテンツの改ざんを可能にする場合があります。  **セキュリティへの影響：攻撃者は、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 Workstation Pro * VMware vCenter Server * VMware Fusion * VMware Telco Cloud Platform * VMware Cloud Foundation * VMware Telco Cloud Infrastructure   **公開日：2025年5月20日  CVSSv3スコア範囲：4.3 – 8.8** |

**サイバーセキュリティアドバイザリ**

アタックサーフェスが拡大し、より洗練された脅威アクターが台頭する中、脆弱性管理はリアクティブな姿勢からプロアクティブで予測的なアプローチへと変化している。この変革には、リスクベースの手法の採用、高度な脅威インテリジェンスの活用、より広範なセキュリティアーキテクチャとの連携が必要です。現代の脆弱性管理は、組織特有の脅威環境を考慮に入れ、それに応じて修復戦略をカスタマイズする必要があります。  
  
そこで、当社のプロアクティブな高度脆弱性管理（AVM）サービスが登場し、リスクベースのアプローチ、資産価値、脆弱性の深刻度、脅威環境に基づく堅牢な脆弱性管理システムの構築を支援します。