

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| 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. | | | | |  |  |  |  | |  |
|  | | | |

|  |
| --- |
| 脆弱性の詳細および解決策： |

**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。**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **VMSA-2025-0010：VMware ESXi、vCenter Server、Workstation および Fusion のアップデートは、複数の脆弱性（CVE-2025-41225、CVE-2025-41226、CVE-2025-41227、CVE-2025-41228）に対応しております。**   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 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 | |
| * サーバー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含まれております。VMware は、本問題の重大度を「重要」な深刻度範囲と評価しており、最大 CVSSv3 基本スコアは 8.8 でございます。**  セキュリティ影響: 十分な権限を持つ攻撃者が本脆弱性を悪用することにより、不正なコマンドを実行される可能性がございます。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ございます。  **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CVEは一般的にシステムの完全性に影響を及ぼし、十分な権限分離が行われていない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）**   * 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ございます。   **説明: VMware ESXi には、ゲストオペレーションを実行する際に発生する、コンテナ内のサービス拒否の脆弱性が存在いたします。VMware は本問題の深刻度を「Moderate」と評価しており、最大 CVSSv3 基本値は 6.8 であると判断しております。**  CVE-2025-41226は、VMware ESXiにおけるサービス拒否（DoS）脆弱性であり、ゲスト操作中にトリガーされ、認証済みユーザーが仮想マシンの可用性を妨害する可能性がございます。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信頼性の低下を引き起こす可能性がございます。  **セキュリティ影響：ゲスト操作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。**  **既知の攻撃ベクター：VM上でゲスト操作権限を有し、すでにvCenter ServerまたはESXiを通じて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に対して、サービス拒否（DoS）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、特定のガイダンスに基づくオプションに起因するサービス拒否の脆弱性が存在いたします。VMware は本問題の深刻度を「Moderate」と評価しており、最大 CVSSv3 基本値は 5.5 でございます。**  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。  **CVE-2025-41227は、VMware ESXi、Workstation、およびFusionに影響を及ぼすサービス拒否（DoS）脆弱性です。この脆弱性により、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性能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。**  **VMware、ESXi および vCenter サーバー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、入力値の検証が不適切であることに起因する、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いたします。VMware は本問題の深刻度を「Moderate（中程度）」と評価しており、最大 CVSSv3 基本値は 4.3 となっております。   **CVE-2025-41228は、VMware ESXiおよびvCenter Serverに存在するリフレクテッドクロスサイトスクリプティング（XSS）の脆弱性であり、不適切な入力検証に起因しております。一般的に、XSS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ございます。**  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、ホスト側においてサービス拒否（DoS）状態を発生させる可能性がございます。本脆弱性はシステムの侵害を許可するものではございませんが、ホスト上で稼働しているワークロードの中断やサービスの信頼性に影響を及ぼす可能性がございます。  **セキュリティ影響: 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へ誘導したりする可能性があります。本脆弱性は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を損なう恐れがあります。**  **影響を受ける製品：**  **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URLパス上のログインページへ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ございます。**   * VMware vCenter サーバ * VMware ESXi * Pro * VMware Fusion * VMware Cloud Foundation * Telco Cloud Platform * 公開日: 2025年5月20日  CVSSv3 スコア範囲: 4.3 – 8.8   **Telco Cloud Infrastructure** |