【医療 ISAC】H-ISAC 脅威速報 – VMWare ディレクトリサービスの重大な脆弱性

おはようございます、医療 ISAC 事務局です。
H-ISAC より VMWare ディレクトリサービスに関する脅威速報を受信しましたので、取り急ぎ会員の皆様に共有いたします。
詳細は下記の H-ISAC 脅威速報（Google 翻訳使用）をご参照ください。

2020 年 4 月 16 日
TLP-WHITE

イベント:
VMWare ディレクトリサービスの重大な脆弱性

概要:
2020 年 4 月 3 日、米国保健福祉省（HHS）のヘルスセクターサイバーセキュリティ調整センター（HC3）は、VMWare ディレクトリサービスに関する重大な脆弱性（VMSA-2020-0006）に関するセクターアラートを公開しました。

分析:
VMWare のディレクトリサービス製品、特にバージョン 6.0 および 6.5 からアップグレードされたバージョン 6.7 のインストールで、非常に重大な脆弱性が検出されました。
VMWare サーバー仮想化システムは、ヘルスケアおよび公衆衛生（HPH）エンティティが IT インフラストラクチャの多くをサポートするために使用している可能性のある、多くの従来の物理コンピューターシステムの仮想化と統合を可能にします。
VMWare のディレクトリサービス製品は、VMware の vCenter Server 製品におけるシングルサインオンサービス（SSO）の中心的なコンポーネント要素です。
この脆弱性を利用して、ネットワークにアクセスできる悪意のある人物が非常に機密性の高い情報を抽出し、他の認証メカニズムを迂回できる可能性があります。

この脆弱性は、VMware ディレクトリサービス（vmdir）に焦点を当てています。
vmdir は VMware の vCenter Server 製品の一部であり、単一のコンソールから仮想化されたホストと仮想マシン（VM）を集中管理します。
特定の条件下では、vmdir は適切なアクセス制御を実装しません。
VMware は、この問題の重大度を重大な重大度の範囲内であると評価し、最大 CVSSv3 ベーススコアは 10 のうち 10 でした。

この脆弱性は、バージョン 6.0 または 6.5 からアップグレードされた vCenter Server バージョン 6.7 インスタンスにのみ影響します。
vCenter Server 6.7（組み込みまたは外部の PSC）のクリーンインストールは影響を受けません。

推奨される緩和策:

- システムログファイルを確認して、VMWare のディレクトリサービスの実装が影響を受けているかどうかを判断します。
- 影響を受けるデプロイメントでは、vmdir サービスがレガシーACL モードが有効になっていることを示すと、ログエントリが作成されます。
- 影響を受けるシステムを VMWare Directory Service バージョン 6.7u3f または 7.0 にアップグレードします。

Health-ISAC メンバーは、Common Vulnerabilities＆Exposures（CVE）とその重要度を引き続き確認および監視して、内部およびリモートシステムのパッチ管理に適切な優先順位が適用されるようにする必要があります。

Health-ISAC は、重要なデータのオフサイトバックアップを維持して、上記のいずれかの CVE が悪用された場合にデータの整合性または可用性が失われるのを防ぐことをメンバーに推奨しています。 ここで利用可能な追加のベストプラクティスについては、「医療業界のサイバーセキュリティプラクティス（HICP）：脅威の管理と患者の保護」を参照してください。

参照資料:

VMware. (April 9 2020). VMware Security Advisories. vmware.com. Accessed 14 April 2020
https://www.vmware.com/security/advisories/VMSA-2020-0006.html

VMware. (May 31 2019). vCenter Single Sign-On Components. VMware.com. Accessed 14 April
https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.install.doc/GUID-90C1E3DC-4397-4BF0-808E-DF3802E56BC6.html

Paganini, P. (April 10 2020). CVE-2020-3952 flaw could allow attackers to hack VMware vCenter Server. Accessed14 April 2020
https://securityaffairs.co/wordpress/101388/security/cve-2020-3952-vmware-vcenter-server.html

Seals, T.(April 10 2020). Critical VMware Bug Opens Up Corporate Treasure to Hackers. Accessed 14 April 2020

https://threatpost.com/critical-vmware-bug-corporate-treasure-hackers/154682/

Olenick, D. (April 13 2020). VMware issues 10.0 CVSS rating on vCenter Server vulnerability. Accessed 14 April 2020
https://www.scmagazine.com/home/security-news/vulnerabilities/vmware-issues-10-0-cvss-rating-on-vcenter-server-vulnerability/

※このレポートは H-ISAC が配信した内容を翻訳システムで日本語に翻訳したものを皆様にお届けしています。
