Your IT Company

Principais Vulnerabilidades e Ameaças (Janeiro/25)

1. Objetivo

Este documento foi desenvolvido e fundamentado nas documentações oficiais do NIST (National Institute Of Standards and Technology), MITRE e CVE.org, que são mundialmente conhecidas na área de cibersegurança como modelos de padronização das melhores práticas de segurança, pesquisa de metodologias de ataques, defesa cibernética e catalogação de novas vulnerabilidades em sistemas operacionais e aplicações.

2. Vulnerabilidades e Ameaças descobertas

2.1. Vulnerabilidade no Oracle VM VirtualBox permite que atacantes elevem privilégios para obter acesso avançado ao sistema

A vulnerabilidade afeta o Oracle VM VirtualBox, um produto da Oracle Virtualization. Ela permite que um atacante com privilégios elevados escape da sandbox, comprometendo a confidencialidade, integridade e disponibilidade dos dados.

A vulnerabilidade identificada como CVE-2025-21571 foi classificada pela Oracle com uma pontuação de nível alto CVSS:3.1:7.3 e ela possui a seguinte descrição. “A vulnerabilidade facilmente explorável permite que um invasor de alto privilégio com logon na infraestrutura em que o Oracle VM VirtualBox é executado comprometa o Oracle VM VirtualBox. Embora a vulnerabilidade esteja no Oracle VM VirtualBox, os ataques podem afetar significativamente produtos adicionais (alteração de escopo). Ataques bem-sucedidos dessa vulnerabilidade podem resultar em criação, exclusão ou modificação não autorizadas, acesso a dados críticos ou a todos os dados acessíveis do Oracle VM VirtualBox, bem como acesso de leitura não autorizado a um subconjunto de dados acessíveis do Oracle VM VirtualBox e capacidade não autorizada de causar uma negação de serviço parcial (DOS parcial) do Oracle VM VirtualBox”. A CVE-2025-21571 ainda não foi avaliada pela NIST.

A falha está presente nas versões do Oracle VirtualBox anteriores às 7.0.24 e 7.1.6. Um atacante com privilégios elevados pode explorar essa vulnerabilidade para escapar do ambiente isolado (sandbox) do VirtualBox, permitindo acesso não autorizado aos dados e potencial controle do sistema hospedeiro.

Exploração

Atualmente, não há evidências de exploração ativa dessa vulnerabilidade, e ainda não foram publicadas provas de conceito. No entanto, dada a gravidade da falha, é fundamental que os usuários adotem medidas proativas para mitigar potenciais riscos.

Mitigação e prevenção

Para reduzir os riscos associados à vulnerabilidade CVE-2025-21571, os usuários e administradores do Oracle VirtualBox devem adotar uma abordagem proativa que inclua as seguintes práticas:

Atualização do Software: A Oracle já disponibilizou patches que corrigem a vulnerabilidade nas versões 7.0.24, 7.1.6 e posteriores do VirtualBox. É essencial que todas as instâncias do software sejam atualizadas imediatamente para as versões corrigidas. Isso garante que a exploração da falha seja mitigada.

Avaliação de Impacto Antes da Atualização: Antes de aplicar os patches, é recomendável realizar uma avaliação de impacto para garantir que os sistemas dependentes do VirtualBox não sofram interrupções após a atualização. Isso pode incluir a execução de testes em ambientes isolados ou de homologação.

Aplicação de Práticas de Segurança no Host e na Rede:

Restringir o acesso às máquinas virtuais através de controles de rede, como firewalls e segmentação de rede, reduzindo a exposição a atacantes externos.

Implementar um modelo de privilégios mínimos, garantindo que apenas usuários autorizados tenham acesso às configurações e operações sensíveis do VirtualBox.

Monitorar logs e eventos do sistema para identificar atividades incomuns ou comportamentos suspeitos que possam indicar tentativas de exploração.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://nvd.nist.gov/vuln/detail/CVE-2025-21571 , https://www.tenable.com/cve/CVE-2025-21571 e https://cyberveille.esante.gouv.fr/alertes/oracle-virtualbox-cve-2025-21571-2025-01-22

2.2. AWS alerta sobre várias vulnerabilidades no Amazon WorkSpaces, Amazon AppStream 2.0 e Amazon DCV

A Amazon Web Services (AWS) abordou recentemente duas vulnerabilidades críticas de segurança que afetam seus populares serviços baseados em nuvem: Amazon WorkSpaces, Amazon AppStream 2.0 e Amazon DCV (Desktop Cloud Visualization).

As vulnerabilidades, identificadas como CVE-2025-0500 e CVE-2025-0501, podem permitir que agentes mal-intencionados executem ataques man-in-the-middle e obtenham acesso não autorizado a sessões remotas.

O CVE-2025-0500, que afeta versões específicas de clientes nativos para o Amazon WorkSpaces (usando o protocolo Amazon DCV), o Amazon AppStream 2.0 e o Amazon DCV, recebeu uma pontuação CVSS v4.0 de 7,7, indicando um alto nível de gravidade.

Essa vulnerabilidade afeta várias versões do cliente em todas as principais plataformas.

Da mesma forma, o CVE-2025-0501 visa especificamente os clientes do Amazon WorkSpaces que utilizam o protocolo PCoIP.

Exploração

CVE-2025-0500

O CVE-2025-0500 afeta os usuários do Amazon WorkSpaces e do Amazon AppStream 2.0 ao utilizar o protocolo Amazon NICE DCV.

Essa vulnerabilidade pode permitir que agentes mal-intencionados executem ataques man-in-the-middle, permitindo o acesso não autorizado a WorkSpaces, AppStream ou sessões DCV remotas.

As versões afetadas por essa vulnerabilidade incluem o cliente Windows 5.20.0 ou anterior do Amazon WorkSpaces, o cliente macOS 5.20.0 ou anterior e o cliente Linux 2024.1 ou anterior.

Além disso, a vulnerabilidade afeta o cliente Windows do Amazon AppStream 2.0 versão 1.1.1326 ou anterior, bem como o cliente Windows do Amazon DCV versão 2023.1.8993 ou anterior, o cliente macOS versão 2023.1.6203 ou anterior e o cliente Linux versão 2023.1.6203 ou anterior para todas as distribuições compatíveis.

CVE-2025-0501

A segunda vulnerabilidade, CVE-2025-0501, aplica-se especificamente ao Amazon WorkSpaces ao usar o protocolo Amazon PCoIP.

Semelhante ao CVE-2025-0500, esse problema pode permitir que invasores executem ataques man-in-the-middle, comprometendo as sessões remotas do WorkSpaces.

As versões afetadas por essa vulnerabilidade incluem o cliente Windows 5.22.0 ou anterior do Amazon WorkSpaces, o cliente macOS 5.22.0 ou anterior, o cliente Linux 2024.5 ou anterior e o cliente Android 5.0.0 ou anterior.

Mitigação e prevenção

CVE-2025-0500

Para resolver essa vulnerabilidade, a AWS recomenda que os usuários atualizem para as seguintes versões ou posteriores: cliente Windows 5.21.0 ou posterior do Amazon WorkSpaces, cliente macOS 5.21.0 ou posterior e cliente Linux 2024.2 ou posterior.

Para o Amazon AppStream 2.0, os usuários devem atualizar para o cliente Windows versão 1.1.1332 ou posterior.

Para o Amazon DCV, as atualizações recomendadas são o cliente Windows versão 2023.1.9127 ou posterior, o cliente macOS versão 2023.1.6703 ou posterior e o cliente Linux versão 2023.1.6703 ou posterior para todas as distribuições compatíveis.

CVE-2025-0501

Para mitigar os riscos associados ao CVE-2025-0501, os usuários são aconselhados a atualizar para as seguintes versões ou posteriores: cliente Windows 5.22.1 ou posterior do Amazon WorkSpaces, cliente macOS 5.22.1 ou posterior, cliente Linux 2024.6 ou posterior e cliente Android 5.0.1 ou posterior.

Recomendações para usuários da AWS

A AWS enfatiza a importância crítica de manter versões de software atualizadas para proteger dados confidenciais e garantir um ambiente de trabalho seguro.

A empresa se comunicou proativamente com seus clientes sobre o fim do suporte para as versões afetadas, reforçando a urgência de os usuários atualizarem.

As organizações que utilizam os serviços da AWS devem adotar as melhores práticas implementando atualizações regularmente e realizando avaliações de vulnerabilidade.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://cybersecuritynews.com/aws-patches-multiple-vulnerabilities e https://gbhackers.com/aws-warns-of-multiple-vulnerabilities/

2.3. Vulnerabilidade no MySQL Server possibilita a elevação de privilégios, permitindo ataques de negação de serviço (DoS)

O MySQL Server, parte do Oracle MySQL, é um sistema de gerenciamento de banco de dados relacional (RDBMS) amplamente utilizado, projetado para armazenar, organizar e recuperar grandes volumes de dados de maneira eficiente. Ele é baseado no modelo cliente-servidor, onde um servidor centralizado gerencia os dados enquanto clientes interagem com ele por meio de conexões de rede.

Recentemente, foi identificada uma vulnerabilidade crítica no MySQL Server da Oracle, registrada como CVE-2025-21559. Essa falha afeta o componente InnoDB nas seguintes versões:

- 8.0.40 e anteriores
- 8.4.3 e anteriores
- 9.1.0 e anteriores

Exploração

A exploração dessa vulnerabilidade é considerada facilmente executável, exigindo privilégios elevados e acesso à rede por meio de múltiplos protocolos. Um atacante bem-sucedido pode explorar a falha para:

Causar a interrupção completa do serviço (DoS – Denial of Service): Travamentos frequentes do MySQL Server.

Obter acesso não autorizado: Realizar operações de atualização, inserção ou exclusão em dados acessíveis pelo servidor.

Embora o impacto sobre a confidencialidade seja limitado, os efeitos sobre a integridade e a disponibilidade são significativos. O CVSS Base Score para essa vulnerabilidade é 5.5, com vetores definidos como:

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

Até o momento, não foi identificada nenhuma prova de conceito (PoC) pública para essa vulnerabilidade, o que pode oferecer uma janela de tempo para mitigação antes que exploits sejam desenvolvidos.

Mitigação e prevenção

A Oracle recomenda enfaticamente que os clientes apliquem os patches de segurança de Atualização suas instâncias do MySQL Server para as versões corrigidas mais recentes, assim que estas estiverem disponíveis.

Para mais detalhes sobre a vulnerabilidade acesse os seguintes links abaixo: https://www.tenable.com/cve/CVE-2025-21559 e https://www.tenable.com/cve/CVE-2025-21559

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

A publicação do documento de Inteligência de Ameaças será realizada quinzenalmente.

Produzido por: Comitê Editorial de Segurança da Service Sec