POC Lançado para VMware Workstation - Against Invaders - Notícias de C

Data: 2025-10-03 05:57:13

Autor: Inteligência Against Invaders

O NCC Group detalhou uma fuga de hóspedes a hospedeiro da VMware, alcançada de uma VM

comprometida por meio de uma falha lógica no manuseio de dispositivos virtuais que permite a

corrupção da memória e a execução de código controlada no processo do host.

A redação mostra um caminho prático de exploração do Usuário Guest de Compromisso de Hospedar, validando o risco do mundo real.

O ataque requer execução dentro de uma VM convidada, mas nenhum privilégio especial de convidado além da capacidade de enviar entradas criadas para a interface VMware Backdoor/RPC, como relatado pelo grupo NCC.

Afetado e impacto

A fuga permite quebrar o isolamento da VM, executar o código arbitrário no contexto do host do processo de hipervisor da estação de trabalho e girar no sistema de arquivos host e VMs adjacentes.

Nos terminais de desenvolvedor de vários VM ou ambientes de laboratório sensíveis, isso permite roubo de dados e movimento lateral.

Tabela cve

Campo	Detalhes
Cve	Escape de convidado para hospedeiro na estação de trabalho VMware
Produtos afetados	VMware Workstation (versões vulneráveis ??específicas por relatório do grupo NCC)
Componente	VMware Backdoor/RPC Virtual Disposition Maniplel Path
CVE IDS	CVE2023-20870/CVE-2023-34044 e CVE-2023-20869

Código POC

Abaixo está um esboço consistente com a descrição de prova de conceito do grupo NCC para defesa educacional e validação em um laboratório controlado. Use apenas para testar o status e as detecções remendadas.

- Estabeleça uma sessão VMware Backdoor/RPC da Guest Userland.

- Envie dois ou mais pacotes RPC com o mesmo SessionID, manipulando o tamanho binário e o deslocamento/tamanho da carga útil para acionar uma escrita fora dos limites na rotina de manuseio do buffer de host.
- Alcançar um substituto de adjacente Memória do host Para redirecionar o fluxo de controle para dados controlados por atacantes.
- Terreva uma carga útil mínima do shell do lado do hospedeiro executado no contexto do processo de estação de trabalho.

Esboço de pseudocódigo de alto nível:

```
// guest-side pseudocode outline open_vmware_backdoor(); uint32_t sid = rp
c_begin_session(); // Packet A: prime host buffer rpc_send(sid, .bin_size
= A_SIZE, .payload_off = OFF_A, .payload_size = SZ_A, .data = bufA); // Pa
cket B: overlapping write to force OOB and corrupt adjacent metadata/code
ptr rpc_send(sid, .bin_size = B_SIZE, .payload_off = OFF_B, .payload_size
= SZ_B, .data = crafted_overlap); // Optional: Packet C to finalize contro
l-flow hijack rpc_send(sid, .bin_size = C_SIZE, .payload_off = OFF_C, .pay
load_size = SZ_C, .data = rop_or_shellcode); // Trigger vulnerable process
ing path rpc_commit(sid);
```

Detalhe da exploração-chave: a reutilização do mesmo SessionID com tamanho/deslocamento de deslocamento criado causa um erro de cálculo de limite de buffer que executa uma escrita fora dos limites no analisador do host, permitindo redirecionamento confiável para o código controlado por atacantes.

Mitigação

- Aplique atualizações de segurança do VMware que remediam o caminho de manuseio de dispositivo virtual/RPC vulnerável.
- Restringir cargas de trabalho não confiáveis ??na estação de trabalho local; VMs de teste de alto risco separadas dos dados sensíveis do host.
- Monitore os processos VMware para criação anormal de processos infantis e acesso a arquivos originários do processo de host da estação de trabalho.
- Aplicar o EDR do host e o controle de aplicativos para restringir o comportamento do processo de hipervisor após a exploração.