Race Conditions - CompTIA Security+ SY0-701 - 2.3

1.Condições de corrida

Uma race condition ocorre quando dois eventos acontecem quase simultaneamente dentro de um aplicativo, e o sistema não consegue lidar corretamente com essa simultaneidade. Desenvolvedores frequentemente tentam evitar esse tipo de problema, mas, em alguns casos, a interação de diferentes processos pode levar a resultados inesperados. Um exemplo comum desse fenômeno é o **Time-Of-Check to Time-Of-Use (TOC/TOU)**, que acontece quando um sistema verifica um determinado valor, mas antes que esse valor seja utilizado, outro processo o altera, causando um comportamento inesperado no software.

Para entender melhor, imagine um sistema bancário onde dois usuários realizam transações simultâneas entre duas contas. Suponha que existam as contas A e B, ambas com saldo inicial de 100 dólares. O primeiro usuário transfere 50 dólares para a conta B e verifica seu saldo atualizado. Em paralelo, um segundo usuário também transfere 50 dólares para a conta B e consulta o saldo. Como o sistema atualiza depósitos imediatamente, ambos os usuários veem que a conta B agora possui 200 dólares. No entanto, ao retirar 50 dólares da conta A, o sistema pode não registrar corretamente a atualização para ambos os usuários, resultando em valores incorretos e um saldo inconsistente.

Race conditions não ocorrem apenas em sistemas financeiros, mas também em dispositivos de grande porte. Em 2004, o **Mars Rover Spirit**, enviado pela NASA a Marte, sofreu um problema crítico devido a uma falha no sistema de arquivos. Para corrigir erros fatais, o software do rover estava programado para reiniciar automaticamente sempre que detectasse falhas. No entanto, como o problema estava no sistema de arquivos, a falha persistia após cada reinicialização, colocando o rover em um **loop infinito de reboot**. Felizmente, os engenheiros conseguiram enviar comandos adicionais para contornar a falha e restaurar o funcionamento do sistema.

Race conditions também podem ser exploradas por atacantes em vulnerabilidades de segurança. No evento **Pwn2Own 2023**, pesquisadores conseguiram explorar um ataque TOC/TOU contra um **Tesla Model 3** através do sistema de infotainment Bluetooth do veículo. Esse ataque permitiu a elevação de privilégios, concedendo aos pesquisadores acesso total ao sistema do carro e garantindo a eles um prêmio de 100 mil dólares, além do próprio Tesla como recompensa.

Esse tipo de falha demonstra como race conditions podem representar riscos tanto para aplicações tradicionais quanto para dispositivos modernos e sistemas críticos. Para mitigar esses problemas, desenvolvedores precisam implementar

mecanismos rigorosos de controle de concorrência, garantindo que múltiplos processos não interfiram entre si de maneira inesperada.