Heathbleed

Como funciona: Heartbleed é uma vulnerabilidade descoberta no OpenSSL, uma biblioteca usada para criptografia na internet. Ela afeta a implementação do protocolo TLS/SSL. O problema está no processo de "heartbeat", um recurso usado para manter uma conexão aberta e verificar se o outro lado da comunicação está ativo.

A vulnerabilidade permite que um invasor envie uma solicitação malformada que pede mais dados do que deveria, o que resulta na exposição de partes da memória do servidor que não deveriam ser acessadas. Esses dados podem incluir informações sensíveis, como chaves de criptografia, senhas, e outras informações confidenciais.

Quando foi detectada: Heartbleed foi detectada em abril de 2014 por Neel Mehta, um pesquisador do Google Security, e pela empresa de segurança Codenomicon. Ela afetava versões do OpenSSL lançadas desde março de 2012.

Como foi explorada: A exploração da vulnerabilidade é relativamente simples. Um invasor pode enviar um "heartbeat" falso com um valor que indica que a resposta deveria conter mais dados do que o necessário. O servidor, por não verificar corretamente o tamanho da mensagem, envia de volta blocos de dados adicionais que podem incluir informações sensíveis. A exploração não deixa rastros nos logs do sistema, o que dificulta a detecção de que o ataque está ocorrendo ou ocorreu.

Como foi corrigida: A correção para a vulnerabilidade foi lançada rapidamente após a descoberta. O OpenSSL lançou uma atualização (versão 1.0.1g) que corrigiu o problema ao verificar corretamente o tamanho dos pacotes de heartbeat. Adicionalmente, muitas organizações que usavam versões vulneráveis tiveram que substituir suas chaves de criptografia e atualizar os certificados digitais para evitar que informações potencialmente comprometidas fossem utilizadas por atacantes.

Vulnerabilidade de software, hardware ou humana? Heartbleed é uma vulnerabilidade de software, especificamente relacionada à implementação defeituosa de um protocolo de comunicação criptografada no OpenSSL.