



**HEARTBLEED**

**Turma:** RSI 1º B

**Nº:** 30156

**Nome:** Pedro Rodrigues

**O que o Heartbleed?**

Heartbleed é um bug na biblioteca de software de criptográfico de OpenSSL, que aos permite atacantes roubar as informações protegidas sob condições normais pela criptografia SSL/TLS usada para proteger a internet. O SSL/ TLS fornece segurança de comunicação e privacidade na Internet para aplicativos como web, email, mensagens instantâneas e redes de privadas virtuais (VPN).



**Como funciona o Heartbleed?**

O bug começou com a validação de entrada incorreta na implementação do OpenSSL, devido aos limites omissos, de verificar os campos de comprimentos e a carga nas solicitações de Hearbeat, além de confiar nos dados recebidos de outras máquinas, a máquina responde por engano e envia de volta os seus próprios dados de memória. Durante um handshake criptografo por TLS, duas máquinas enviam mensagens de Hearbeat, uma resposta precisa conter a cópia da carga útil da solicitação de Heatbeat. Quando uma mensagem de solicitação de Heartbeat é recebida, grava o conteúdo da carga útil em sua memória e copia o conteúdo de volta em resposta. O openSSL aloca memória para a resposta com base no tamanho e depois copia a carga útil para resposta usando memcpy().

Os atacantes podem enviar solicitações de Heartbeat com o valor do campo lengh maior que o tamanho real da carga útil. Os processos do OpenSSL na máquina estão respondendo ás solicitações de Heartbeat não verificaram se o tamanho da carga útil é igual ao especificado no campo de comprimento. Assim, a máquina copia os dados extras que residem na memória após a carga na resposta, portanto, os bytes extras são dados adicionais no processo remoto.

 