Sistemas Afetados

Todos os sistemas e aplicativos que utilizam o Secure Socket Layer (SSL) 3.0 com cifras de modo de encadeamento de blocos de criptografia (CBC) podem ser vulneráveis. No entanto, o ataque POODLE (Enchimento da Oracle em Criptografia Legada com Downgrade) demonstra essa vulnerabilidade usando navegadores da Web e servidores da Web, que é um dos cenários de exploração mais prováveis.

Algumas implementações TLS (Transport Layer Security) também são vulneráveis ​​ao ataque POODLE.

visão global

A US-CERT está ciente de uma vulnerabilidade de projeto encontrada na maneira como o **SSL 3.0** manipula o preenchimento do modo de cifra de bloco. O ataque POODLE demonstra como um invasor pode explorar essa vulnerabilidade para descriptografar e extrair informações de dentro de uma transação criptografada.

Descrição

A vulnerabilidade do SSL 3.0 deriva da forma como os blocos de dados são criptografados sob um tipo específico de algoritmo de criptografia dentro do protocolo SSL. **O ataque POODLE aproveita o recurso de negociação de versão do protocolo incorporado ao SSL / TLS para forçar o uso do SSL 3.0 e, em seguida, aproveita essa nova vulnerabilidade** para descriptografar o conteúdo selecionado na sessão SSL. A descriptografia é feita byte por byte e irá gerar um grande número de conexões entre o cliente e o servidor.

Embora o SSL 3.0 seja um padrão de criptografia antigo e geralmente tenha sido substituído pelo TLS, a maioria das implementações de SSL / TLS permanece compatível com o SSL 3.0 para interoperar com sistemas legados no interesse de uma experiência de usuário tranquila. Mesmo que um cliente e um servidor suportem uma versão do TLS, o conjunto de protocolos SSL / TLS permite a negociação de versão de protocolo (sendo referida como a “**dança de downgrade**” em outros relatórios). **O ataque POODLE aproveita o fato de que, quando uma tentativa de conexão segura falha, os servidores retornam aos protocolos mais antigos, como o SSL 3.0. Um invasor que pode disparar uma falha de conexão pode forçar o uso do SSL 3.0 e tentar o novo ataque**. [1]

**Duas outras condições devem ser atendidas para executar com sucesso o ataque POODLE: 1) o atacante deve ser capaz de controlar partes do lado do cliente da conexão SSL (variando o comprimento da entrada) e 2) o invasor deve ter visibilidade do resultado texto cifrado. A maneira mais comum de atingir essas condições seria atuar como Man-in-the-Middle (MITM),** exigindo uma forma totalmente separada de ataque para estabelecer esse nível de acesso.

Essas condições dificultam um pouco a exploração bem-sucedida. Ambientes que já estão em risco acima da média para ataques MITM (como WiFi público) removem alguns desses desafios.

Em 8 de dezembro de 2014, foi divulgado publicamente [2,3,4] que algumas implementações de TLS também são vulneráveis ​​ao ataque POODLE.

Impacto

O ataque POODLE pode ser usado contra qualquer sistema ou aplicativo que suporte SSL 3.0 com criptografias de modo CBC. Isso afeta a maioria dos navegadores e sites atuais, mas também inclui qualquer software que faça referência a uma biblioteca SSL / TLS vulnerável (por exemplo, OpenSSL) ou implemente o próprio pacote de protocolos SSL / TLS. Ao explorar essa vulnerabilidade em um provável cenário baseado na Web, um invasor pode obter acesso a dados confidenciais transmitidos na sessão da Web criptografada, como senhas, cookies e outros tokens de autenticação que podem ser usados ​​para obter acesso mais completo a um site ( representando esse usuário, acessando o conteúdo do banco de dados etc.).

Solução

Atualmente, não há correção para a própria vulnerabilidade do SSL 3.0, pois o problema é fundamental para o protocolo; No entanto, desabilitar o suporte ao SSL 3.0 nas configurações do sistema / aplicativo é a solução mais viável atualmente disponível.

Alguns dos mesmos pesquisadores que descobriram a vulnerabilidade também desenvolveram uma correção para uma das condições de pré-requisito; TLS\_FALLBACK\_SCSV é uma extensão de protocolo que impede que invasores MITM sejam capazes de forçar um downgrade de protocolo. O OpenSSL adicionou suporte para TLS\_FALLBACK\_SCSV às suas versões mais recentes e recomendou as seguintes atualizações: [5]

    Usuários do OpenSSL 1.0.1 devem atualizar para o 1.0.1j.

    Os usuários do OpenSSL 1.0.0 devem atualizar para 1.0.0o.

    Os usuários do OpenSSL 0.9.8 devem atualizar para 0.9.8zc.

Os clientes e servidores precisam suportar o TLS\_FALLBACK\_SCSV para evitar ataques de downgrade.

Outras implementações do SSL 3.0 provavelmente também são afetadas pelo POODLE. Entre em contato com seu fornecedor para obter detalhes. Informações adicionais sobre fornecedores podem estar disponíveis na entrada do National Vulnerability Database (NVD) para CVE-2014-3566 [6] ou no CERT Vulnerability Note VU # 577193. [7]

Implementações de TLS vulneráveis ​​precisam ser atualizadas. CVE ID atribuições e informações do fornecedor também estão disponíveis no NVD. [8]

Referências