Vulnerabilidade fraca do modo de CBC do protocolo SSLv3 e TLSv1

Índice

Introdução

Este documento descreve como desabilitar cifras do modo do Cipher Block Chaining (CBC) na ferramenta de segurança do email de Cisco (ESA). Uma auditoria de Segurança/varredura pôde relatar que um ESA tem uma vulnerabilidade fraca do modo de CBC do protocolo v1 da Segurança da camada do secure sockets layer (SSL) v3/Transport (TLS).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em AsyncOS para a Segurança do email (alguma revisão), Cisco ESA, e um ESA virtual.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

- A conformidade padrão da segurança de dados da indústria do cartão do pagamento (PCI DSS) exige cifras CBC ser desabilitada.
- Uma auditoria de Segurança/varredura identificou uma vulnerabilidade potencial com protocolos SSL v3/TLS v1 que usam cifras do modo de CBC.

  Dica: O 3.0 da versão de SSL (RFC-6101) é um Obsoleto e um protocolo inseguro. Há uma vulnerabilidade em SSLv3 CVE-2014-3566 conhecido como o Oracle do estofamento no ataque da criptografia do legado Downgraded (CANICHE), a identificação de bug Cisco CSCur27131. A recomendação é desabilitar SSL v3 quando você mudar as cifras e usar o TLS somente, e seleciona o option 3 (TLS v1). Reveja a identificação de bug Cisco fornecida CSCur27131 para detalhes completos.

Os protocolos SSL v3 e TLS v1 são usados a fim fornecer a integridade, a autenticidade, e a privacidade a outros protocolos tais como o HTTP e o Lightweight Directory Access Protocol (LDAP). Proporcionam estes serviços com o uso da criptografia para a privacidade, dos Certificados x509 para a autenticidade, e da funcionalidade de criptografia de sentido único para a integridade. A fim cifrar dados, o SSL e o TLS podem usar as cifras de bloco que são os algoritmos de criptografia que podem cifrar somente um bloco fixo de dados originais a um bloco cifrado do mesmo tamanho. Note que estas cifras obterão sempre o mesmo bloco resultante para o mesmo bloco original de dados. A fim conseguir a diferença na saída, a saída da criptografia é XORed com contudo um outro bloco do mesmo tamanho referido como os vetores de inicialização (iv). O CBC usa um IV para o bloco inicial e o resultado do bloco precedente para cada bloco subsequente a fim obter a diferença na saída da criptografia da cifra de bloco.

Na aplicação SSL v3 e TLS v1, o uso bem escolhido do modo de CBC era deficiente porque o tráfego inteiro compartilha de uma sessão CBC com um conjunto único de IV iniciais. O resto dos IV é, como mencionado previamente, resultados da criptografia dos blocos precedentes. Os IV subsequentes estão disponíveis aos eavesdropperes. Isto permite um atacante com a capacidade de injetar o tráfego arbitrário no córrego do texto simples (para ser cifrado pelo cliente) a fim verificar sua suposição do texto simples que precede o bloco injetado. Se a suposição dos atacantes está correta, a seguir a saída da criptografia é a mesma para dois blocos.

Para baixos dados da entropia, é possível supor relativamente o bloco do texto simples com um número baixo de tentativas. Por exemplo, para os dados que têm 1000 possibilidades, o número de tentativas pode ser 500.

Requisitos

Há as várias requisições que devem ser cumpridas para que a façanha trabalhe:

1. A conexão SSL/TLS deve usar uma das cifras da criptografia do bloco que usam o modo de CBC, tal como o DES ou o AES. Os canais que usam cifras de córrego tais como o RC4 não são sujeitos à falha. Uma grande proporção de conexões SSL/TLS usa o RC4.
2. A vulnerabilidade pode somente ser explorada por alguém que intercepta dados na conexão SSL/TLS, e igualmente envia ativamente dados novos nessa conexão. A exploração da falha faz com que a conexão SSL/TLS seja terminada. O atacante deve continuar a monitorar e usar novas conexões até que bastante dados estejam recolhidos para decifrar a

mensagem.
3. Desde que a conexão é terminada cada vez, o cliente SSL/TLS deve poder continuar a restabelecer o suficiente o canal SSL/TLS para que a mensagem seja decifrada.
4. O aplicativo deve enviar novamente os mesmos dados em cada conexão SSL/TLS que cria e o ouvinte deve poder encontrá-lo no fluxo de dados. Protocolos como IMAP/SSL que têm um grupo fixo de mensagens para entrar a reunião esta exigência. O web geral que consulta não faz.

Ameaça

A vulnerabilidade CBC é uma vulnerabilidade com TLS v1. Esta vulnerabilidade realizou-se na existência desde 2004 adiantado, e foi resolvida em umas versões mais atrasadas do v1.2 TLS v1.1 e TLS.

Antes de AsyncOS 9.6 para a Segurança do email, o ESA utiliza o v1.0 TLS e as cifras do modo de CBC. Com liberação de AsyncOS 9.6, o ESA introduz o v1.2 TLS. Ainda, as cifras do modo de CBC podem ser desabilitadas, e somente as cifras RC4 podem ser usadas que não são sujeitas à falha.

Além, se SSLv2 é permitido isto pode provocar um falso positivo para esta vulnerabilidade. É muito importante que o SSL v2 esteja desabilitado.

Solução

Desabilite cifras do modo de CBC a fim deixar somente as cifras RC4 permitidas. Ajuste o dispositivo para usar somente TLS v1, ou o v1.2 TLS v1/TLS:

1. Entre ao CLI.
2. Incorpore o **sslconfig do** comando.
3. Incorpore o comando **GUI**.
4. Escolha o número de opção 3 para “TLS v1", ou como catalogado em AsyncOS 9.6" TLS v1/TLS v1.2".
5. Incorpore esta cifra:`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. Incorpore o comando: **DE ENTRADA**.
7. Escolha o número de opção 3 para “TLS v1", ou como catalogado em AsyncOS 9.6" TLS v1/TLS v1.2".
8. Incorpore esta cifra:`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
9. Inscreva o comando outbound.
10. Escolha o número de opção 3 para “TLS v1", ou como catalogado em AsyncOS 9.6" TLS v1/TLS v1.2".
11. Incorpore esta cifra:`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
12. A imprensa **entra** até que você retorne à alerta do hostname.
13. Inscreva o comando commit.
14. Finalize que compromete suas mudanças.

O ESA está configurado agora para apoiar somente o v1.2 TLS v1, ou TLSv1/TLS, com cifras

RC4 quando recusar todos os filtros CBC.

Está aqui a lista de cifras usadas quando você ajusta RC4:-SSLv2. Note que não há nenhuma cifra do modo de CBC na lista.

```
ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
EXP-ADH-RC4-MD5 SSLv3 Kx=DH(512) Au=None Enc=RC4(40) Mac=MD5 export
EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
```

Quando esta façanha for do interesse muito baixo devido a suas complexidade e exigências explorar, o desempenho destas etapas é uma grande proteção para a prevenção de façanhas possíveis, assim como para passar varreduras restritas da Segurança.

Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems