Vulnérabilité faible de mode CBC SSLv3 et TLSv1 Protocol

Contenu

Introduction

Ce document décrit comment désactiver le bloc de chiffrement enchaînant des chiffrements du mode (CBC) sur l'appliance de sécurité du courrier électronique de Cisco (ESA). Un audit de sécurité/balayage pourrait signaler qu'un ESA a une vulnérabilité faible de mode CBC de Secure Sockets Layer (SSL) v3/Transport Layer Security (TLS) v1 Protocol.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur AsyncOS pour la sécurité du courrier électronique (toute révision), Cisco ESA, et un ESA virtuel.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

- La conformité standard de protection des données de secteur de carte de paiement (norme PCI DSS) exige des chiffrements CBC d'être désactivés.
- Un audit de sécurité/balayage a identifié une vulnérabilité potentielle avec les protocoles SSL v3/TLS v1 qui utilisent des chiffrements de mode CBC.

  Conseil : La version 3.0 (RFC-6101) SSL est une Désuet(e) et un protocole non sécurisé. Il y a une vulnérabilité dans SSLv3 CVE-2014-3566 connu sous le nom de compléter Oracle sur l'attaque existante de cryptage Downgraded (CANICHE), l'ID de bogue Cisco CSCur27131. La recommandation est de désactiver SSL v3 tandis que vous changez les chiffrements et le TLS d'utilisation seulement, et sélectionne l'option 3 (TLS v1). Passez en revue l'ID de bogue Cisco fourni CSCur27131 pour les détails complets.

Des protocoles SSL v3 et de TLS v1 sont utilisés afin de fournir l'intégrité, l'authenticité, et l'intimité à d'autres protocoles tels que le HTTP et le Protocole LDAP (Lightweight Directory Access Protocol). Ils fournissent à ces services l'utilisation du cryptage pour l'intimité, des Certificats x509 pour l'authenticité, et de la fonctionnalité de cryptage à sens unique pour l'intégrité. Afin de chiffrer des données, le SSL et le TLS peuvent utiliser les chiffres par bloc qui sont des algorithmes de chiffrement qui peuvent chiffrer seulement un bloc fixe de données d'origine à un bloc chiffré de la même taille. Notez que ces chiffrements obtiendront toujours le même bloc en résultant pour le même bloc d'origine de données. Afin de réaliser la différence dans la sortie, la sortie du cryptage est XORed avec encore un autre bloc de la même taille désignée sous le nom des vecteurs d'initialisation (iv). Utilisations une CBC IV pour le bloc initial et le résultat du bloc précédent pour chaque bloc ultérieur afin d'obtenir la différence dans la sortie du cryptage de chiffre par bloc.

Dans l'implémentation SSL v3 et de TLS v1, l'utilisation de mode CBC de choix était pauvre parce que les partages du trafic entiers une session CBC avec une série unique d'IVs initial. Le reste de l'IVs sont, comme mentionné précédemment, des résultats du cryptage des blocs précédents. L'IVs ultérieur sont à la disposition des oreilles indiscrètes. Ceci permet à un attaquant avec la capacité pour injecter le trafic arbitraire dans le flot de texte brut (être chiffré par le client) afin de vérifier leur conjecture du texte brut qui précède le bloc injecté. Si la conjecture d'attaquants est correcte, alors la sortie du cryptage est identique pour deux blocs.

Pour de basses données d'entropie, il est possible de deviner le bloc de texte brut avec relativement un nombre peu élevé de tentatives. Par exemple, pour les données qui ont 1000 possibilités, le nombre de tentatives peut être 500.

Conditions requises

Il y a des plusieurs conditions qui doivent être répondues pour que l'exploit fonctionne :

1. La connexion SSL/TLS doit utiliser un des chiffrements de cryptage de bloc qui utilisent le mode CBC, tel que le DES ou l'AES. Les canaux qui utilisent des chiffrements de flux tels que le RC4 ne sont pas sujets à l'imperfection. Une grande proportion de connexions SSL/TLS utilisent le RC4.
2. La vulnérabilité peut seulement être exploitée par quelqu'un qui intercepte des données sur la connexion SSL/TLS, et envoie également activement de nouvelles données sur cette connexion. L'exploitation de l'imperfection cause la connexion SSL/TLS d'être terminée.

L'attaquant doit continuer à surveiller et utiliser de nouvelles connexions jusqu'à ce qu'assez de données soient recueillies pour déchiffrer le message.
3. Puisque la connexion est terminée chaque fois, le client SSL/TLS doit pouvoir continuer à rétablir le canal SSL/TLS assez longtemps pour que le message soit déchiffré.
4. L'application doit renvoyer les mêmes données sur chaque connexion SSL/TLS qu'elle crée et l'auditeur doit pouvoir la localiser dans le flux de données. Protocoles comme IMAP/SSL qui ont un ensemble fixe de messages pour ouvrir une session le rassemblement cette condition requise. La navigation web générale ne fait pas.

Menace

La vulnérabilité CBC est une vulnérabilité avec le TLS v1. Cette vulnérabilité a été en existence depuis début 2004, et a été résolue dans les versions ultérieures du TLS v1.1 et du TLS v1.2.

Avant AsyncOS 9.6 pour la sécurité du courrier électronique, l'ESA des chiffrements utilise du TLS v1.0 et CBC mode. Avec la release d'AsyncOS 9.6, l'ESA introduit le TLS v1.2. Toujours, des chiffrements de mode CBC peuvent être désactivés, et on peut utiliser seulement les chiffrements RC4 qui ne sont pas sujets à l'imperfection.

En outre, si SSLv2 est activé ceci peut déclencher un faux positif pour cette vulnérabilité. Il est très important que SSL v2 soit désactivé.

Solution

Désactivez les chiffrements de mode CBC afin de laisser seulement les chiffrements RC4 activés. Placez le périphérique pour utiliser seulement le TLS v1, ou le TLS v1/TLS v1.2 :

1. Procédure de connexion au CLI.
2. Écrivez le **sslconfig de** commande.
3. Écrivez le **GUI de** commande.
4. Choisissez l'option le numéro 3 pour le « TLS v1", ou comme répertorié dans AsyncOS 9.6" le TLS v1/TLS v1.2".
5. Écrivez ce chiffrement :`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. Sélectionnez la commande : **D'ARRIVÉE**.
7. Choisissez l'option le numéro 3 pour le « TLS v1", ou comme répertorié dans AsyncOS 9.6" le TLS v1/TLS v1.2".
8. Écrivez ce chiffrement :`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
9. Sélectionnez la commande **SORTANTE**.
10. Choisissez l'option le numéro 3 pour le « TLS v1", ou comme répertorié dans AsyncOS 9.6" le TLS v1/TLS v1.2".
11. Écrivez ce chiffrement :`MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
12. La presse **entrent** jusqu'à ce que vous reveniez à la demande d'adresse Internet.
13. Entrez dans la **validation de** commande.
14. Finalize commettant vos modifications.

L'ESA est maintenant configuré pour prendre en charge seulement le TLS v1, ou le TLSv1/TLS

v1.2, avec les chiffrements RC4 tandis qu'il rejette tous les filtres CBC.

Voici la liste de chiffrements utilisés quand vous placez RC4:-SSLv2. Notez qu'il n'y a aucun chiffrement de mode CBC dans la liste.

```
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
```

Tandis que cette exploit est concernée très bas dû à sa complexité et conditions requises d'exploiter, la représentation de ces étapes est une grande sauvegarde pour la prévention des exploits possibles, aussi bien que pour passer des balayages stricts de Sécurité.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems