Schwachstelle des SSL v3- und TLS v1-Protokolls im CBC-Modus

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Cipher Block Chaining (CBC) Mode Cipher auf der Cisco E-Mail Security Appliance (ESA) deaktiviert wird. Ein Sicherheitsprüfer/-scan kann angeben, dass eine ESA über eine Schwachstelle im CBC-Modus Secure Sockets Layer (SSL) v3/Transport Layer Security (TLS) v1 Protocol verfügt.

> **Achtung**: Wenn Sie älteren Code von AsyncOS für Email Security ausführen, wird ein Upgrade auf Version 11.0.3 oder höher empfohlen. In den Cisco Email Security-Versionshinweisen finden Sie aktuelle Versionen und Informationen zu unseren Produkten. Wenn Sie weitere Unterstützung bei Upgrades oder bei der Deaktivierung von Chiffren benötigen, öffnen Sie bitte ein Support-Ticket.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf AsyncOS für E-Mail-Sicherheit (beliebige Version), einer Cisco ESA und einer virtuellen ESA.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

- Die Einhaltung des PCI DSS (Payment Card Industry Data Security Standard) erfordert die Deaktivierung von CBC-Chiffren.
- Eine Sicherheitsprüfung/Prüfung hat eine potenzielle Schwachstelle mit SSL v3/TLS v1-Protokollen identifiziert, die CBC-Moduschiffren verwenden.

  Tipp: SSL Version 3.0 (RFC-6101) ist ein veraltetes und unsicheres Protokoll. Eine Schwachstelle in SSLv3 CVE-2014-3566, bekannt als Padding Oracle On Downgraded Legacy Encryption (POODLE)-Angriff, Cisco Bug-ID CSCur27131. Es wird empfohlen, SSL v3 zu deaktivieren, während Sie die Chiffren ändern und nur TLS verwenden, und Option 3 (TLS v1) auszuwählen. Ausführliche Informationen finden Sie in der angegebenen Cisco Bug-ID CSCur27131.

SSL v3- und TLS v1-Protokolle werden verwendet, um anderen Protokollen wie HTTP und LDAP (Lightweight Directory Access Protocol) Integrität, Authentizität und Datenschutz zu bieten. Sie bieten diese Dienste mit Verschlüsselung für den Datenschutz, x509-Zertifikaten für die Authentizität und unidirektionaler Verschlüsselungsfunktionalität für die Integrität. Um Daten zu verschlüsseln, können SSL und TLS Blockchiffren verwenden, bei denen es sich um Verschlüsselungsalgorithmen handelt, die nur einen festen Block mit Originaldaten in einen verschlüsselten Block derselben Größe verschlüsseln können. Beachten Sie, dass diese Chiffren immer denselben Ergebnisblock für denselben ursprünglichen Datenblock erhalten. Um einen Unterschied in der Ausgabe zu erzielen, wird die Ausgabe der Verschlüsselung XORed mit einem weiteren Block derselben Größe, genannt Initialisierungsvektoren (IV), ausgegeben. Der CBC verwendet für den ursprünglichen Block eine IV und für jeden nachfolgenden Block das Ergebnis des vorherigen Blocks, um die Differenz in der Ausgabe der Verschlüsselung der Blockchiffre zu ermitteln.

Bei der Implementierung von SSL v3 und TLS v1 war die Wahl des CBC-Modus mangelhaft, da der gesamte Datenverkehr eine CBC-Sitzung mit einem einzigen Satz anfänglicher IVs gemeinsam nutzt. Die übrigen IVs sind, wie bereits erwähnt, das Ergebnis der Verschlüsselung der vorherigen Blöcke. Die nachfolgenden IV stehen den Lauschköpfen zur Verfügung. Dies ermöglicht es einem Angreifer, beliebigen Datenverkehr in den Klartext-Stream einzufügen (der vom Client verschlüsselt werden soll), um seine Einschätzung des Klartextes zu überprüfen, der dem infizierten Block vorangeht. Wenn die Vermutung des Angreifers richtig ist, ist die Verschlüsselungsausgabe für zwei Blöcke gleich.

Bei Daten mit niedriger Entropie ist es möglich, den Textblock mit relativ wenigen Versuchen zu erraten. Bei Daten mit 1.000 Möglichkeiten kann die Anzahl der Versuche beispielsweise 500 sein.

Anforderungen

Es gibt mehrere Anforderungen, die erfüllt werden müssen, damit der Exploit funktioniert:

1. Die SSL/TLS-Verbindung muss eine der Verschlüsselungscodes verwenden, die den CBC-Modus verwenden, z. B. DES oder AES. Kanäle, die Streamchiffren wie RC4 verwenden, unterliegen nicht dem Fehler. Ein großer Teil der SSL/TLS-Verbindungen verwendet RC4.
2. Die Schwachstelle kann nur von jemandem ausgenutzt werden, der Daten in der SSL/TLS-Verbindung abfängt und darüber hinaus aktiv neue Daten über diese Verbindung sendet. Die Ausnutzung des Fehlers führt dazu, dass die SSL/TLS-Verbindung beendet wird. Der

Angreifer muss weiterhin neue Verbindungen überwachen und verwenden, bis genügend Daten gesammelt wurden, um die Nachricht zu entschlüsseln.
3. Da die Verbindung jedes Mal beendet wird, muss der SSL/TLS-Client in der Lage sein, den SSL/TLS-Kanal weiter so lange wiederherzustellen, dass die Nachricht entschlüsselt werden kann.
4. Die Anwendung muss dieselben Daten für jede von ihr erstellte SSL/TLS-Verbindung erneut senden, und der Listener muss in der Lage sein, diese Daten im Datenstrom zu lokalisieren. Protokolle wie IMAP/SSL, die über einen festen Satz von Nachrichten für die Anmeldung verfügen, erfüllen diese Anforderung. Allgemeine Internetnutzung nicht.

Bedrohung

Die CBC-Schwachstelle ist eine Schwachstelle von TLS v1. Diese Schwachstelle besteht seit Anfang 2004 und wurde in späteren Versionen von TLS v1.1 und TLS v1.2 behoben.

Vor AsyncOS 9.6 für E-Mail-Sicherheit verwendet die ESA TLS v1.0- und CBC-Moduschiffren. Mit der Einführung von AsyncOS 9.6 führt die ESA TLS v1.2 ein. Dennoch können CBC-Moduschiffren deaktiviert werden, und es können nur RC4-Chiffren verwendet werden, die nicht fehlerhaft sind.

Wenn SSLv2 aktiviert ist, kann dies außerdem einen Fehlalarm für diese Schwachstelle auslösen. Es ist sehr wichtig, dass SSL v2 deaktiviert wird.

Lösung

> **Achtung**: Wenn Sie älteren Code von AsyncOS für Email Security ausführen, wird ein Upgrade auf Version 11.0.3 oder höher empfohlen. In den Cisco Email Security-Versionshinweisen finden Sie aktuelle Versionen und Informationen zu unseren Produkten. Wenn Sie weitere Unterstützung bei Upgrades oder bei der Deaktivierung von Chiffren benötigen, öffnen Sie bitte ein Support-Ticket.

Deaktivieren Sie die CBC-Moduschiffren, damit nur RC4-Chiffren aktiviert bleiben. Stellen Sie das Gerät so ein, dass nur TLS v1 oder TLS v1/TLS v1.2 verwendet wird:

1. Melden Sie sich bei der CLI an.
2. Geben Sie den Befehl **sslconfig ein**.
3. Geben Sie den Befehl **GUI ein**.
4. Wählen Sie Option Nr. 3 für "TLS v1" aus, oder wie in AsyncOS 9.6 "TLS v1/TLS v1.2" aufgeführt.
5. Geben Sie diesen Verschlüsselungscode ein:
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. Geben Sie den Befehl ein: **EINGEHEND**.
7. Wählen Sie Option Nr. 3 für "TLS v1" aus, oder wie in AsyncOS 9.6 "TLS v1/TLS v1.2" aufgeführt.
8. Geben Sie diesen Verschlüsselungscode ein:
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`

9. Geben Sie den Befehl **OUTBOUND ein**.
10. Wählen Sie Option Nr. 3 für "TLS v1" aus, oder wie in AsyncOS 9.6 "TLS v1/TLS v1.2" aufgeführt.
11. Geben Sie diesen Verschlüsselungscode ein:
    `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
12. Drücken Sie **die Eingabetaste**, bis Sie zur Eingabeaufforderung für den Hostnamen zurückkehren.
13. Geben Sie den Befehl **commit ein**.
14. Beenden Sie das Commit Ihrer Änderungen.

Die ESA ist jetzt so konfiguriert, dass sie nur TLS v1 oder TLSv1/TLS v1.2 mit RC4-Chiffren unterstützt, während sie alle CBC-Filter deaktiviert.

Hier ist die Liste der Chiffren verwendet, wenn Sie RC4:-SSLv2. Beachten Sie, dass die Liste keine CBC-Moduschiffren enthält.

```
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
```

Diese Exploits sind zwar aufgrund ihrer Komplexität und der zu nutzenden Anforderungen nur von sehr geringem Wert, doch die Durchführung dieser Schritte ist ein großer Sicherheitsfaktor, um mögliche Exploits zu verhindern und strenge Sicherheitsscans zu durchlaufen.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems