SSL v3 en TLS v1 Protocol Weken CBC-modus

Inhoud

Inleiding

Dit document beschrijft hoe u Cipher Block Chaining (CBC) mode-filters kunt uitschakelen op de Cisco e-mail security applicatie (ESA). Een veiligheidscontrole/scan kan melden dat een ESA een Secure Socket Layer (SSL) v3/Transport Layer Security (TLS) v1 Protocol Week CBC Mode kwetsbaarheid heeft.

> **Let op**: Als u een oudere code van AsyncOS voor e-mailbeveiliging gebruikt, wordt het aanbevolen om een upgrade naar versie 11.0.3 of nieuwer uit te voeren. Bekijk de opmerkingen van Cisco Email Security release voor onze nieuwste versies en informatie. Als u verdere assistentie nodig hebt bij upgrades of het uitschakelen van cifen, open dan een ondersteuningscase.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op AsyncOS voor e-mail security (elke herziening), een Cisco ESA, en een virtuele ESA.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

- Om aan de eisen van de gegevensbeveiligingsstandaard (PCI DSS) te voldoen, moeten CBC-cips worden uitgeschakeld.
- Een veiligheidscontrole/scan heeft een mogelijke kwetsbaarheid geïdentificeerd met SSL v3/TLS v1-protocollen die CBC Mode CIFERS gebruiken.

  Tip: SSL versie 3.0 (RFC-6101) is een verouderd en onveilig protocol. Er is een kwetsbaarheid in SSLv3 CVE-2014-3566, dat staat bekend als Padding Oracle On Downgraded Legacy Encryption (POODLE)-aanval, Cisco bug ID CSCur27131. De aanbeveling is om SSL v3 uit te schakelen terwijl u alleen de telefoons wijzigt en TLS-apparatuur gebruikt, en optie 3 (TLS v1). Bekijk de meegeleverde Cisco bug-ID CSCur27131 voor volledige informatie.

SSL v3 en TLS v1-protocollen worden gebruikt om integriteit, authenticiteit en privacy te bieden aan andere protocollen zoals HTTP en Light Directory Access Protocol (LDAP). Zij leveren deze diensten met behulp van encryptie voor privacy, x509 certificaten voor authenticiteit en eenrichtingscoderingsfunctionaliteit voor integriteit. Om gegevens te versleutelen kunnen SSL en TLS bloktelefoons gebruiken die encryptie-algoritmen zijn die alleen een vast blok van oorspronkelijke gegevens kunnen versleutelen naar een gecodeerd blok van dezelfde grootte. Merk op dat deze ciphers altijd hetzelfde resulterende blok voor hetzelfde originele blok gegevens zullen verkrijgen. Om een verschil in de output te bereiken, wordt de output van de encryptie XORed met een ander blok van dezelfde grootte, de initialisatiesectoren genoemd (IV). CBC gebruikt één IV voor het eerste blok en het resultaat van het vorige blok voor elk volgend blok om het verschil in de output van de encryptie van het blokalgoritme te verkrijgen.

Bij SSL v3 en TLS v1 implementatie was het gebruik van de CBC-modus slecht omdat het gehele verkeer één CBC-sessie deelt met één set initiële IV's. De rest van de IV's zijn, zoals eerder vermeld, het resultaat van de encryptie van de vorige blokken. De volgende IV's zijn beschikbaar voor de afluisteraars. Dit staat een aanvaller toe met de mogelijkheid om willekeurig verkeer in de gewone-tekststroom te injecteren (te versleutelen door de client) om hun schatting van de gewone tekst die aan het geïnjecteerde blok voorafgaat te verifiëren. Als de aanslagplegers' raad correct is, dan is de output van de encryptie hetzelfde voor twee blokken.

Voor lage entropiegegevens is het mogelijk om het gewone tekstvak te raden met een relatief laag aantal pogingen. Bijvoorbeeld, voor gegevens die 1000 mogelijkheden hebben, kan het aantal pogingen 500 zijn.

Vereisten

Er zijn verschillende eisen waaraan moet worden voldaan om de exploitatie te laten werken:

1. De SSL/TLS-verbinding moet een van de blokencryptieschakelaars gebruiken die de modi CBC, zoals DES of AES, gebruiken. Kanalen die stream ciphers zoals RC4 gebruiken zijn niet onderworpen aan de fout. Een groot deel van SSL/TLS-verbindingen maakt gebruik van RC4.
2. De kwetsbaarheid kan alleen worden uitgebuit door iemand die gegevens over de SSL/TLS-verbinding onderschept, en kan ook actief nieuwe gegevens over die verbinding versturen. De exploitatie van de fout veroorzaakt dat de SSL/TLS-verbinding wordt beëindigd. De aanvaller moet nieuwe verbindingen blijven bewaken en gebruiken tot er genoeg gegevens zijn verzameld om het bericht te decrypteren.
3. Aangezien de verbinding elke keer wordt beëindigd, moet de SSL/TLS-client in staat zijn om

het SSL/TLS-kanaal lang genoeg te herstellen zodat het bericht kan worden gedecrypteerd.
4. De toepassing moet dezelfde gegevens op elke SSL/TLS-verbinding opnieuw verzenden die het creëert en de luisteraar moet het in de gegevensstroom kunnen vinden. Protocollen als IMAP/SSL met een vaste set berichten die u wilt inloggen, voldoen aan deze eis. Algemene webbrowsing doet dat niet.

dreun

De kwetsbaarheid van de CBC is een kwetsbaarheid voor TLS v1. Deze kwetsbaarheid bestaat sinds begin 2004 en werd opgelost in latere versies van TLS v1.1 en TLS v1.2.

Voorafgaand aan AsyncOS 9.6 voor e-mail security gebruikt het ESR TLS v1.0- en CBC-modems. Met de release van AsyncOS 9.6 introduceert het ESR TLS v1.2. Toch kunnen er ciphers in de CBC-modus worden uitgeschakeld en kunnen alleen RC4-microfoons worden gebruikt die niet aan de fout zijn onderworpen.

Als SSLv2 is geactiveerd, kan dit bovendien een valse positieve waarde voor deze kwetsbaarheid veroorzaken. Het is erg belangrijk dat SSL v2 wordt uitgeschakeld.

Oplossing

> **Let op**: Als u een oudere code van AsyncOS voor e-mailbeveiliging gebruikt, wordt het aanbevolen om een upgrade naar versie 11.0.3 of nieuwer uit te voeren. Bekijk de opmerkingen van Cisco Email Security release voor onze nieuwste versies en informatie. Als u verdere assistentie nodig hebt bij upgrades of het uitschakelen van cifen, open dan een ondersteuningscase.

CBC-modems uitschakelen om alleen RC4-telefoons in te schakelen. Stel het apparaat in om alleen TLS v1 of TLS v1/TLS v1.2 te gebruiken:

1. Meld u aan bij de CLI.
2. Voer de opdrachtregel **in**.
3. Voer de opdracht **GUI in**.
4. Kies optie nummer 3 voor "TLS v1", of zoals vermeld in AsyncOS 9.6 "TLS v1/TLS v1.2".
5. Voer dit algoritme in:
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. Typ de opdracht: **BINNENKOMEN**.
7. Kies optie nummer 3 voor "TLS v1", of zoals vermeld in AsyncOS 9.6 "TLS v1/TLS v1.2".
8. Voer dit algoritme in:
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
9. Typ de opdracht **OUTBOUND**.
10. Kies optie nummer 3 voor "TLS v1", of zoals vermeld in AsyncOS 9.6 "TLS v1/TLS v1.2".
11. Voer dit algoritme in:
    `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
12. Druk op **ENTER** totdat u terugkeert naar de hostname melding.
13. Voer de opdracht **in**.

14. Voltooi het doorvoeren van je wijzigingen.

De ESA is nu zo ingesteld dat alleen TLS v1 of TLSv1/TLS v1.2 ondersteunen met RC4-filters terwijl de CBC-filters worden uitgeschakeld.

Hier is de lijst met ciphers die gebruikt worden wanneer u RC4:-SSLv2 instelt. Let op dat er geen CBC mode ciphers in de lijst zijn.

```
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
```

Hoewel deze exploitatie van zeer weinig belang is vanwege de complexiteit ervan en de eisen om deze te exploiteren, is de uitvoering van deze stappen een belangrijke waarborg voor het voorkomen van mogelijke exploitatie en voor het doorvoeren van strenge veiligheidsscans.

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems