Vermijd de kwetsbaarheid van POODLE- en POODLE-BITEN bij gebruik van ASA en AnyConnect

Inhoud

Inleiding

Dit document beschrijft wat u moet doen om het opvullen van Oracle op gedowngraded Legacy Encryption (POODLE) kwetsbaarheid te voorkomen wanneer u adaptieve security applicaties (ASA's) en AnyConnect voor Secure Socket Layer (SSL) connectiviteit gebruikt.

Achtergrondinformatie

De kwetsbaarheid van POODLE beïnvloedt bepaalde implementaties van het protocol van de Veiligheid van de Transport Layer 1 (TLSv1) en kon een niet-echt bevonden, afstandsaanvaller aan toegang tot gevoelige informatie toestaan.

De kwetsbaarheid is het gevolg van ongeschikte opvulling van het blok die in TLSv1 is geïmplementeerd wanneer u de modus Cipher Block Chaining (CBC) gebruikt. Een aanvaller zou de kwetsbaarheid kunnen uitbuiten om een 'orakle padding' zijkanaalaanval op het cryptografische bericht uit te voeren. Een succesvolle exploitatie zou de aanvaller toegang kunnen geven tot gevoelige informatie.

Probleem

ASA staat inkomende SSL verbindingen in twee vormen toe:

1. Clientloze WebVPN
2. AnyConnect-client

Geen van de TLS-implementaties op de ASA of de AnyConnect-client is echter beïnvloed door POODLE. In plaats daarvan wordt de SSLv3-implementatie beïnvloed zodat alle klanten (browser of AnyConnect) die SSLv3 onderhandelen, gevoelig zijn voor deze kwetsbaarheid.

> **Voorzichtig:** POODLE BITES hebben echter wel invloed op de TLSv1 op de ASA. Raadpleeg voor meer informatie over getroffen producten en fixes CVE-2014-8730.

Oplossing

Cisco heeft deze oplossingen voor dit probleem geïmplementeerd:

1. Alle versies van AnyConnect die eerder werden ondersteund (onderhandeld) SSLv3 zijn afgekeurd en de versies die beschikbaar zijn voor download (zowel v3.1x als v4.0) zullen niet onderhandelen over SSLv3 zodat ze niet gevoelig zijn voor het probleem.

2. De standaardinstelling van het standaardprotocol van de ASA is gewijzigd van SSLv3 in TLSv1.0 zodat zolang de inkomende verbinding van een client is die TLS ondersteunt, dat is wat er zal worden onderhandeld.

3. ASA kan handmatig worden ingesteld om alleen specifieke SSL-protocollen met deze opdracht te accepteren:

   ssl server-version

   Zoals vermeld in oplossing 1, onderhandelt geen van de momenteel ondersteunde AnyConnect-clients meer over SSLv3, zodat de client geen verbinding meer maakt met een ASA die met een van deze opdrachten is geconfigureerd:
   ```
   ssl server-version sslv3
   ssl server-version sslv3-only
   ```

   Voor implementaties die gebruik maken van de v3.0.x- en v3.1.x AnyConnect-versies die zijn gedegradeerd (die allemaal AnyConnect-bouwversies PRE 3.1.05182 zijn) en waarin SSLv3-onderhandeling specifiek wordt gebruikt, is de enige oplossing echter het gebruik van SSLv3 te elimineren of een upgrade van de client te overwegen.

4. De eigenlijke oplossing voor POODLE BITES (Cisco bug-ID CSCus08101) wordt alleen in de nieuwste interim-versies geïntegreerd. U kunt upgraden naar een ASA-versie die de oplossing voor het probleem heeft. De eerste beschikbare versie op Cisco Connection Online (CCO) is versie 9.3(2.2).

   De eerste vaste ASA-software-releases voor deze kwetsbaarheid zijn als volgt:
   8.2 Treinen: 8.2.5.558.4 Treinen: 8.4.7.269.0 Treinen: 9.0.4.299.1 trein: 9.1.69.2 Treintrein: 9.2.3.39.3 Treinbouw: 9.3.2.2

TLSv1.2

- De ASA ondersteunt TLSv1.2 vanaf softwareversie 9.3(2).
- AnyConnect versie 4.x-clients ondersteunen TLSv1.2.

Dit betekent:

- Als u Clientloze WebVPN gebruikt, kan elke ASA die deze versie van de software of hoger heeft, met TLSv1.2 onderhandelen.

- Als u de AnyConnect-client gebruikt om TLSv1.2 te gebruiken, moet u een upgrade uitvoeren

naar versie 4.x-client.

Gerelateerde informatie

- CVE-2014-8730
- Cisco bug-id CSC51375
- Cisco bug-id CSCur4276
- Technische ondersteuning en documentatie – Cisco Systems