Evitare le vulnerabilità dei bit di barboncino e barboncino quando si usano ASA e AnyConnect

Sommario

Introduzione

In questo documento viene descritto come evitare la vulnerabilità Padding Oracle On Downgraded Legacy Encryption (POODLE) quando si usano le appliance ASA (Adaptive Security Appliance) e AnyConnect per la connettività SSL (Secure Sockets Layer).

Premesse

La vulnerabilità POODLE influisce su alcune implementazioni del protocollo TLSv1 (Transport Layer Security versione 1) e potrebbe consentire a un utente non autenticato e remoto di accedere a informazioni riservate.

La vulnerabilità è dovuta all'implementazione non corretta del riempimento a blocchi tramite cifratura in TLSv1 quando si utilizza la modalità CBC (Cipher Block Chaining). Un utente non autorizzato potrebbe sfruttare la vulnerabilità per eseguire un attacco del canale laterale "oracle padding" al messaggio crittografico. Un exploit riuscito potrebbe consentire all'aggressore di accedere alle informazioni riservate.

Problema

L'appliance ASA consente le connessioni SSL in arrivo in due forme:

1. WebVPN senza client
2. Client AnyConnect

Tuttavia, nessuna delle implementazioni TLS sull'appliance ASA o sul client AnyConnect è influenzata da POODLE. L'implementazione SSLv3 viene invece interessata, in modo che tutti i client (browser o AnyConnect) che negoziano SSLv3 siano soggetti a questa vulnerabilità.

> **Attenzione:** Tuttavia, le PUNTURE DI BARBONCINO influiscono su TLSv1 sull'appliance ASA. Per ulteriori informazioni sui prodotti interessati e sulle correzioni, fare riferimento a CVE-2014-8730.

Soluzione

Cisco ha implementato queste soluzioni al problema:

1. Tutte le versioni di AnyConnect che in precedenza supportavano (negoziate) SSLv3 sono state dichiarate obsolete e le versioni disponibili per il download (v3.1x e v4.0) non negozieranno SSLv3, quindi non saranno soggette al problema.

2. L'impostazione del protocollo predefinito dell'ASA è stata modificata da SSLv3 a TLSv1.0 in modo che venga negoziata solo se la connessione in ingresso proviene da un client che supporta TLS.

3. L'ASA può essere configurata manualmente per accettare solo protocolli SSL specifici con questo comando:

   `ssl server-version`

   Come accennato nella soluzione 1, nessuno dei client AnyConnect attualmente supportati negozia più il protocollo SSLv3, quindi il client non riuscirà a connettersi ad alcuna appliance ASA configurata con uno dei seguenti comandi:

   ```
   ssl server-version sslv3
   ssl server-version sslv3-only
   ```

   Tuttavia, per le distribuzioni che usano le versioni v3.0.x e v3.1.x di AnyConnect deprecate (tutte le versioni delle build AnyConnect precedenti alla 3.1.05182) e in cui viene usata specificamente la negoziazione SSLv3, l'unica soluzione è eliminare l'uso di SSLv3 o considerare un aggiornamento del client.

4. La correzione attuale per POODLE BITES (Cisco bug ID CSCus08101) verrà integrata solo nelle ultime versioni provvisorie. È possibile eseguire l'aggiornamento a una versione ASA che disponga della funzionalità corretta per risolvere il problema. La prima versione disponibile su Cisco Connection Online (CCO) è la versione 9.3(2.2).

   Le prime versioni software ASA corrette per questa vulnerabilità sono le seguenti:
   8.2 Treno: 8.2.5.558.4 Treno: 8.4.7.269.0 Treno: 9.0.4.299.1 Treno: 9.1.69.2 Treno: 9.2.3.39.3 Treno: 9.3.2.2

TLSv1.2

- L'ASA supporta TLSv1.2 a partire dalla versione software 9.3(2).
- Tutti i client AnyConnect versione 4.x supportano TLSv1.2.

Ciò significa:

- Se si usa una WebVPN senza client, qualsiasi appliance ASA che esegue questa versione del software o una versione successiva può negoziare TLSv1.2.

- Se si usa il client AnyConnect, per usare TLSv1.2, è necessario aggiornare i client alla

versione 4.x.

Informazioni correlate

- CVE-2014-8730
- ID bug Cisco CSCug51375
- ID bug Cisco CSCur42776
- Documentazione e supporto tecnico – Cisco Systems