Soluzioni ASA BEAST Vulnerability

Sommario

[Introduzione](#)
[Problema](#)
[Impatto utente](#)
[Soluzione](#)

Introduzione

In questo documento viene descritta una vulnerabilità del software Cisco Adaptive Security Appliance (ASA) che consente a utenti non autorizzati di accedere ai contenuti protetti. Vengono inoltre descritte le soluzioni per questo problema.

Problema

La vulnerabilità del browser Exploit Against SSL/TLS (BEAST) viene sfruttata da un utente non autorizzato per leggere in modo efficace il contenuto protetto tramite il concatenamento del vettore di inizializzazione (IV) in modalità di crittografia CBC (Cipher Block Chaining) con un attacco di testo normale noto.

L'attacco utilizza uno strumento che sfrutta una vulnerabilità nel protocollo TLSv1 (Transport Layer Security Version 1) ampiamente utilizzato. La questione non ha radici nel protocollo in sé, ma piuttosto nelle suite di cifratura che usa. TLSv1 e Secure Sockets Layer versione 3 (SSLv3) favoriscono le cifrature CBC, dove si verifica l'attacco Oracle Padding.

Impatto utente

Come indicato dall'indagine sull'implementazione SSL Pulse, creata dal Trustworthy Internet Movement, oltre il 75% dei server SSL è esposto a questa vulnerabilità. Tuttavia, la logistica associata allo strumento BEAST è piuttosto complicata. Per utilizzare BEAST per intercettare il traffico, l'aggressore deve essere in grado di leggere e inserire i pacchetti molto rapidamente. Questo potenzialmente limita le destinazioni effettive per un attacco BESTIA. Ad esempio, un attacco BESTIA può efficacemente catturare il traffico casuale in un hotspot WIFI o dove tutto il traffico Internet è bloccato da un numero limitato di gateway di rete.

Soluzione

BEAST è uno sfruttamento della debolezza nel cifrario che viene utilizzato dal protocollo. Dato che

influisce sulla cifratura CBC, la soluzione originale per questo problema era passare alla cifratura RC4. Tuttavia, le debolezze nel Key Scheduling Algorithm dell'articolo RC4 pubblicato nel 2013 rivelano che anche RC4 aveva una debolezza che lo rendeva inadatto.

Per risolvere questo problema, Cisco ha implementato le due correzioni seguenti per l'appliance ASA:

- ID bug Cisco CSCts83720: *Aggiornamento a TLS 1.1/1.2*

  Aggiornare e usare TLS 1.1/1.2. Il limite di questa soluzione è che si applica solo alle piattaforme ASA 5500-X. L'hardware di crittografia sulle piattaforme ASA legacy (ASA 5505 e ASA serie 5500) non supporta TLSv1.2. Di conseguenza, non è possibile risolvere il problema per queste piattaforme.

  A causa delle limitazioni del protocollo, non è disponibile alcuna soluzione per SSLv3 o TLSv1.0; tuttavia, la maggior parte dei browser moderni ha implementato diversi modi di mitigazione.

- ID bug Cisco CSCuc85781: *Randomizzazione cookie WebVPN*

  Per le versioni del software ASA che non supportano TLSv1.2, Cisco ha reso i cookie casuali con questa correzione per ridurre il rischio. Questo non previene completamente gli attacchi BESTIA, ma aiuta a mitigarli.

  Suggerimento: l'unico modo per essere completamente protetti dalla vulnerabilità della BESTIA è usare TLSv1.2. È simile ai cifrari. Cisco continua ad aggiungere codifiche più recenti e più robuste, mentre le codifiche meno recenti potrebbero presentare problemi noti (ad esempio, RC4). Pertanto, Cisco consiglia di passare ai protocolli e alle cifrature più recenti.