Configurazione della selezione del resolver DNS in iOS 14 e macOS 11

Sommario

Introduzione

Questo documento descrive le modifiche apportate a Umbrella dagli aggiornamenti iOS 14 e macOS 11 che includono il supporto per il DNS crittografato.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Security Connector (CSC)
- RC (Umbrella Roaming Client) macOS
- Client AnyConnect (AC) macOS

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Apple ha annunciato il rilascio di iOS 14 il 16 settembre 2020. Tra le altre modifiche, iOS 14 e macOS 11 includono il supporto per il DNS crittografato e la possibilità per i proprietari di dominio di designare un resolver DNS a loro scelta. Questa modifica ha un effetto diretto sulla capacità di Umbrella di risolvere alcuni nomi di dominio, il che significa che le regole e la segnalazione per quei domini sarebbero influenzati.

Le modifiche in iOS 14 e macOS 11 hanno 3 effetti principali:

1. Gli utenti possono specificare un resolver DoH a livello di sistema in grado di eseguire l'override del resolver DNS impostato da DHCP o RA.

2. I proprietari dei domini possono designare i resolver DoH che possono sostituire il resolver DNS impostato da DHCP o RA per le query eseguite per il proprio dominio.

3. Le app possono specificare un resolver DoH in grado di eseguire l'override del resolver DNS impostato da DHCP o RA per le query eseguite dalla loro app. Umbrella non ha la visibilità su quali app stanno facendo così.

Con questi aggiornamenti, Apple non ha incluso un meccanismo per individuare un resolver crittografato in esecuzione sullo stesso IP del resolver di rete con provisioning, il che significa che le reti che inoltrano query ai resolver Umbrella non possono eseguire l'aggiornamento al servizio DoH di Umbrella all'indirizzo doh.umbrella.com.

A partire dal 1 ottobre 2020, Umbrella impedisce la scoperta del resolver DoH che sono stati designati dai proprietari di dominio, che impedisce a tali domini di bypassare la protezione Umbrella. Umbrella non può impedire gli effetti #1 e #3 a meno che un client Umbrella non sia installato sul dispositivo. I clienti che necessitano di protezione da tali effetti possono valutare l'opportunità di bloccare gli IP di provider DoH noti, come descritto in questo articolo.

Per maggiori dettagli sulle modifiche apportate a iOS 14 e macOS 11, continuare a leggere questo articolo.

Impatto per gli utenti Umbrella

Cisco Security Connector (CSC)

Il dispositivo iOS che utilizza CSC non può essere interessato da questa modifica, in quanto utilizza il meccanismo proxy DNS di Apple che ha la priorità sul meccanismo di rilevamento del resolver iOS.

RC (Umbrella Roaming Client) macOS

macOS RC può essere influenzato da questa modifica, in quanto macOS RC attualmente esegue un proxy DNS su localhost, che viene visualizzato da macOS come un resolver non crittografato. RC utilizza DNSCrypt per comunicare con i resolver Umbrella.

Umbrella ha fornito supporto per l'imposizione dell'individuazione DoH nel modulo AnyConnect Roaming Security (vedere AC di seguito) che utilizza il provider proxy DNS Apple per controllare il DNS. Al momento non è previsto che questo supporto venga incluso nella RC. I pacchetti Umbrella sono concessi in licenza per AC. Vedi il nostro articolo.

Client AnyConnect (AC) macOS

I dispositivi macOS che utilizzano l'AC non possono essere interessati da questa modifica, in quanto attualmente utilizzano il meccanismo proxy DNS di Apple che ha la priorità sul meccanismo di rilevamento del resolver di macOS.

Dispositivi iOS o macOS dietro un'appliance virtuale (VA)

Questa modifica può influire su iOS o macOS in cui non è installato CSC, RC o AC. Tali dispositivi dietro un VA possono quindi inviare query direttamente ai server DoH configurati, ignorando l'appliance virtuale.

Dispositivi iOS o macOS dietro una rete registrata

iOS o macOS che non hanno CSC, RC o AC installato non sono interessati da questa modifica. Tali dispositivi dietro una rete registrata possono quindi inviare query direttamente ai server DoH configurati, ignorando il resolver locale o Umbrella.

Umbrella e DNS crittografato

Umbrella supporta pienamente l'uso di DNS crittografati e iniziative per promuovere l'uso di DNS crittografati. I resolver Umbrella hanno supportato DNSCrypt come mezzo per crittografare il traffico DNS dal 2011, e tutto il software client Umbrella supporta l'uso di DNSCrypt e lo utilizza nelle loro configurazioni predefinite. Inoltre, da febbraio 2020 è supportato DNS over HTTPS (DoH).

Umbrella esegue inoltre la convalida DNSSEC sulle query inviate alle autorità upstream al fine di garantire l'integrità dei dati per tutti i record presenti nella cache.

Modifiche DNS dettagliate in iOS 14 e macOS 11

iOS 14 e macOS 11 introducono un nuovo meccanismo per la selezione di un resolver DNS. Mentre i clienti che richiedono dettagli specifici possono confermare con Apple, Cisco è consapevole del meccanismo che è possibile selezionare un resolver DNS con la priorità descritta di seguito:

1. Risoluzione delle zone di test del portale captive che utilizzano il resolver DNS fornito dalla rete

2. Configurazioni di proxy VPN o DNS (ad esempio Cisco Security Connector per iOS) e resolver DNS impostati da criteri aziendali (ad esempio MDM o OTA). Per informazioni dettagliate sull'impostazione dei criteri DNS, rivolgersi al fornitore MDM.

3. Resolver crittografati a livello di sistema configurati direttamente dai proprietari dei dispositivi

4. Resolver crittografati designati dai proprietari del dominio

5. Risolutore crittografato designato dalle app

6. Resolver non crittografati (come i resolver specificati tramite DHCP o RA)

In particolare, riteniamo che i numeri 3, 4 e 5 siano modifiche significative alla selezione del resolver che possono avere un impatto diretto sulla capacità degli amministratori Umbrella di applicare pienamente l'uso dei resolver Umbrella sulle loro reti.

Resolver crittografati a livello di sistema

Gli utenti possono installare un'app del profilo di configurazione da un provider DNS che consente loro di configurare un resolver crittografato a livello di sistema. Questo resolver può essere utilizzato per tutte le query, indipendentemente dal resolver DNS specificato dalla rete tramite DHCP o RSA.

Al momento, l'unico metodo noto per impedire l'utilizzo di questi resolver per i dispositivi non gestiti è bloccare gli IP dei provider DoH noti presso il firewall. In questo modo, l'utente del dispositivo iOS riceverà un avviso e il dispositivo non potrà eseguire il fallback a DNS non crittografato, ovvero non sarà in grado di risolvere i nomi host DNS.

Resolver crittografati designati dai proprietari del dominio

Il proprietario di una zona DNS può designare un resolver specifico da utilizzare per la risoluzione della zona. In iOS 14 e macOS 11, è possibile designare solo resolver DoH. Questa designazione viene effettuata utilizzando un tipo di record DNS dedicato (tipo 65, denominato "HTTPS") e convalidato da DNSSEC o da URI noti.

Poiché tali designazioni determinerebbero l'esclusione delle query da Umbrella, i resolver Umbrella restituirebbero una risposta REFUSED per le query per il tipo di record DNS HTTPS, ovvero tali designazioni non verrebbero individuate.

Risolutore crittografato designato dalle app

L'autore di un'applicazione può specificare un resolver crittografato di fallback se non viene individuato alcun altro resolver crittografato in uno dei meccanismi con priorità più alta. Questo resolver può essere utilizzato solo se l'alternativa consiste nell'utilizzare il resolver non crittografato impostato da DHCP o RA.

Al momento, l'unico metodo noto per impedire l'utilizzo di questi resolver per i dispositivi non gestiti è bloccare gli IP dei provider DoH noti presso il firewall. Non è ancora noto se iOS possa utilizzare il DNS non crittografato in uno scenario di questo tipo.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).