DNS Resolver Selection configureren in iOS 14 en macOS 11

Inhoud

Inleiding

Dit document beschrijft wijzigingen in Umbrella van iOS 14- en macOS 11-updates die ondersteuning voor gecodeerde DNS bevatten.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Apple kondigde de release van iOS 14 aan op 16 september 2020. Onder andere veranderingen, iOS 14 en macOS 11 bevatten ondersteuning voor gecodeerde DNS, en de mogelijkheid voor domeineigenaren om een DNS-resolver van hun keuze aan te wijzen. Deze wijziging heeft een direct effect op het vermogen van Umbrella om sommige domeinnamen op te lossen, wat betekent dat het beleid en de rapportage voor die domeinen zouden worden beïnvloed.

De veranderingen in iOS 14 en macOS 11 hebben 3 primaire effecten:

1. Gebruikers kunnen een DoH-resolver voor het hele systeem opgeven die de DNS-resolver kan overschrijven die is ingesteld door DHCP of RA.

2. Domeineigenaars kunnen DoH-resolvers aanwijzen die de DNS-resolver kunnen overschrijven die is ingesteld door DHCP of RA voor query's die voor hun domein zijn gemaakt.

3. Apps kunnen een DoH-resolver opgeven die de DNS-resolver kan overschrijven die is ingesteld door DHCP of RA voor query's die zijn gemaakt vanuit hun app. Umbrella heeft geen zicht op welke apps dat doen.

Met deze updates heeft Apple geen mechanisme opgenomen om een gecodeerde resolver te ontdekken die op hetzelfde IP als de network provisioned resolver draait, wat betekent dat netwerken die query's doorsturen naar de Umbrella resolvers niet kunnen upgraden naar Umbrella's DoH-service op doh.umbrella.com.

Met ingang van 1 oktober 2020 voorkomt Umbrella de ontdekking van DoH-resolvers die zijn aangewezen door domeineigenaren, waardoor die domeinen de Umbrella-bescherming niet kunnen omzeilen. Umbrella kan effecten #1 en #3 niet voorkomen, tenzij een Umbrella-client op het apparaat is geïnstalleerd. Klanten die bescherming tegen deze effecten nodig hebben, kunnen overwegen om de IP's van bekende DoH-providers te blokkeren, zoals beschreven in dit artikel.

Voor meer informatie over de veranderingen in iOS 14 en macOS 11, lees je dit artikel.

Gevolgen voor paraplu-gebruikers

Cisco Security Connector (CSC)

iOS-apparaten die de CSC gebruiken, kunnen niet worden beïnvloed door deze wijziging, omdat het gebruik maakt van het DNS-proxymechanisme van Apple dat prioriteit heeft boven het detectiemechanisme voor de resolver van iOS.

macOS Umbrella Roaming Client (RC)

macOS-apparaten die de RC gebruiken, kunnen door deze wijziging worden beïnvloed, omdat de macOS RC momenteel een DNS-proxy op localhost uitvoert, die door macOS wordt gezien als een niet-gecodeerde resolver. De RC gebruikt DNSCrypt om te communiceren met de Umbrella resolvers.

Umbrella heeft ondersteuning geleverd voor het afdwingen van DoH-detectie in onze AnyConnect Roaming Security Module (zie AC hieronder) die gebruik maakt van de Apple DNS Proxy Provider om DNS te beheren. Het is niet de bedoeling dat deze ondersteuning op dit moment in de RC wordt opgenomen. Paraplupakketten zijn gelicentieerd voor AC. Zie ons artikel.

macOS AnyConnect-client (AC)

macOS-apparaten die de wisselstroomadapter gebruiken, kunnen niet worden beïnvloed door deze wijziging, omdat ze momenteel het DNS-proxy-mechanisme van Apple gebruiken dat prioriteit heeft boven het detectiemechanisme voor de resolver van macOS.

iOS- of macOS-apparaten achter een Virtual Appliance (VA)

iOS of macOS die geen CSC, RC of AC hebben geïnstalleerd, kunnen door deze wijziging worden beïnvloed. Dergelijke apparaten achter een VA kunnen daarom query's rechtstreeks naar geconfigureerde DoH-servers verzenden, waarbij het virtuele apparaat wordt omzeild.

iOS- of macOS-apparaten achter een geregistreerd netwerk

iOS of macOS die geen CSC, RC of AC hebben geïnstalleerd, worden niet beïnvloed door deze wijziging. Dergelijke apparaten achter een geregistreerd netwerk kunnen daarom query's rechtstreeks naar geconfigureerde DoH-servers verzenden, waarbij de lokale resolver of Umbrella wordt omzeild.

Paraplu en gecodeerde DNS

Umbrella ondersteunt volledig het gebruik van versleutelde DNS en initiatieven om het gebruik van versleutelde DNS te bevorderen. De Umbrella resolvers ondersteunen DNSCrypt sinds 2011 als een middel om DNS-verkeer te versleutelen en alle Umbrella-clientsoftware ondersteunt het gebruik van DNSCrypt en gebruikt het in hun standaardconfiguraties. Daarnaast ondersteunen we sinds februari 2020 DNS over HTTPS (DoH).

Umbrella voert daarnaast DNSSEC-validatie uit op vragen die naar upstream-autoriteiten worden verzonden om de gegevensintegriteit voor alle records in onze cache te waarborgen.

Gedetailleerde DNS-wijzigingen in iOS 14 en macOS 11

iOS 14 en macOS 11 introduceren een nieuw mechanisme voor het selecteren van een DNS-resolver. Terwijl klanten die specifieke details nodig hebben, dit met Apple kunnen bevestigen, is Cisco's begrip van het mechanisme dat een DNS-resolver kan worden geselecteerd met de prioriteit die hier wordt beschreven:

1. Resolutie van testzones voor captive portal met behulp van de DNS-resolver die via het netwerk wordt geleverd

2. VPN- of DNS-proxyconfiguraties (zoals de Cisco Security Connector voor iOS) en DNS-resolvers die zijn ingesteld door bedrijfsbeleid (zoals MDM of OTA). (Raadpleeg uw MDM-leverancier voor meer informatie over het instellen van DNS-beleid)

3. Systeembrede gecodeerde resolvers die rechtstreeks door apparaateigenaars worden geconfigureerd

4. Versleutelde resolvers aangewezen door domeineigenaren

5. Versleutelde resolver aangewezen door apps

6. Niet-versleutelde resolvers (zoals resolvers die via DHCP of RA worden gespecificeerd)

In het bijzonder beschouwen we de nummers 3, 4 en 5 als belangrijke wijzigingen in de selectie van oplossers die een directe invloed kunnen hebben op het vermogen van overkoepelende beheerders om het gebruik van de overkoepelende oplossers op hun netwerken volledig af te dwingen.

Systeembrede gecodeerde resolvers

Gebruikers kunnen een configuratieprofiel-app van een DNS-provider installeren waarmee ze een gecodeerde resolver voor het hele systeem kunnen configureren. Deze resolver kan voor alle query's worden gebruikt, ongeacht de DNS-resolver die door het netwerk via DHCP of RA is opgegeven.

Momenteel is de enige bekende methode om het gebruik van deze resolvers voor onbeheerde apparaten te voorkomen, het blokkeren van de IP's van bekende DoH-providers bij de firewall. Dit kan resulteren in een waarschuwing voor de gebruiker van het iOS-apparaat en het apparaat kan niet terugvallen op niet-gecodeerde DNS, wat betekent dat het niet in staat is om DNS-hostnamen op te lossen.

Gecodeerde resolvers die zijn aangewezen door domeineigenaren

De eigenaar van een DNS-zone kan een specifieke resolver aanwijzen die moet worden gebruikt voor het oplossen van de zone. In iOS 14 en macOS 11 kunnen alleen DoH-resolvers worden aangewezen. Deze aanduiding wordt gemaakt met behulp van een speciaal DNS-recordtype (type 65, genaamd "HTTPS") en gevalideerd door DNSSEC of bekende URI's.

Aangezien dergelijke aanduidingen zouden resulteren in query's die Umbrella omzeilen, retourneren de Umbrella-resolvers een GEWEIGERD antwoord voor query's voor het HTTPS DNS-recordtype, wat betekent dat dergelijke aanduidingen niet worden ontdekt.

Versleutelde resolver aangewezen door apps

Een app-maker kan een fallback gecodeerde resolver opgeven als er geen andere gecodeerde

resolver wordt ontdekt in een van de mechanismen met hogere prioriteit. Deze resolver kan alleen worden gebruikt als het alternatief zou zijn om de niet-versleutelde resolver te gebruiken die is ingesteld door DHCP of RA.

Momenteel is de enige bekende methode om het gebruik van deze resolvers voor onbeheerde apparaten te voorkomen, het blokkeren van de IP's van bekende DoH-providers bij de firewall. Het is nog niet bekend of iOS in een dergelijk scenario kan terugvallen op onversleutelde DNS.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.