在iOS 14和macOS 11中配置DNS解析程式選擇

目錄

簡介

本文檔介紹iOS 14和macOS 11更新中包括對加密DNS支援的更改。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全聯結器(CSC)
- macOS雨傘漫遊使用者端(RC)
- macOS AnyConnect客戶端(AC)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

蘋果公司於2020年9月16日發佈了iOS 14。在其他更改中，iOS 14和macOS 11包含對加密DNS的支援，以及域所有者指定其選擇的DNS解析器的能力。此更改對Umbrella解析某些域名的能力有直接影響，這意味著這些域的策略和報告將受到影響。

iOS 14和macOS 11中的更改有3個主要影響：

1.使用者可以指定系統範圍的DoH解析程式，該解析程式可以覆蓋DHCP或RA設定的DNS解析程式。

2.域所有者可以指定DoH解析器，該解析器可以覆蓋由DHCP或RA為其域進行的查詢設定的DNS解析器。

3.應用可以指定一個DoH解析程式，該解析程式可以覆蓋由DHCP或RA為其應用進行的查詢設定的DNS解析程式。Umbrella無法檢視哪些應用正在這樣做。

通過這些更新，Apple沒有包括發現加密解析程式的機制，該解析程式運行在與網路調配的解析程式相同的IP上，這意味著將查詢轉發到Umbrella解析程式的網路無法升級到Umbrella的DoH服務(doh.umbrella.com)。

截至2020年10月1日，Umbrella阻止發現由域所有者指定的DoH解析程式，防止這些域繞過Umbrella保護。#1除非裝置上安裝了Umbrella客戶端，否則Umbrella無法阻止影響和#3。需要針對這些影響提供保護的客戶可以考慮如本文所述阻止已知的DoH提供商的IP。

有關iOS 14和macOS 11更改的完整詳細資訊，請繼續閱讀本文內容。

對Umbrella使用者的影響

思科安全聯結器(CSC)

使用CSC的iOS裝置不會受到此更改的影響，因為它使用蘋果的DNS代理機制，其優先順序高於iOS的解析程式發現機制。

macOS雨傘漫遊使用者端(RC)

使用RC的macOS裝置可能會受到此更改的影響，因為macOS RC當前在localhost上運行DNS代理，而macOS將其視為未加密的解析程式。RC使用DNSCrypt與Umbrella解析器通訊。

Umbrella在我們的AnyConnect漫遊安全模組（請參閱下面的AC）中提供了對DoH發現的強制支援，該模組利用Apple DNS代理提供程式控制DNS。此支援目前不計畫包括在RC中。Umbrella軟體包授權用於AC。請參閱我們的文章。

macOS AnyConnect客戶端(AC)

使用AC的MacOS裝置不能受到此更改的影響，因為它們當前使用的是優先於MacOS的解析程式發現機制的Apple DNS代理機制。

虛擬裝置(VA)後面的iOS或macOS裝置

未安裝CSC、RC或AC的iOS或macOS可能會受到此更改的影響。因此，VA後面的此類裝置可以繞過虛擬裝置，將查詢直接傳送到已配置的DoH伺服器。

註冊網路後面的iOS或macOS裝置

未安裝CSC、RC或AC的iOS或macOS不受此更改的影響。因此，註冊網路後的此類裝置可以繞過本地解析程式或Umbrella，直接將查詢傳送到已配置的DoH伺服器。

Umbrella和加密的DNS

Umbrella完全支援使用加密的DNS以及推動使用加密DNS的計畫。自2011年以來，Umbrella解析器支援DNSCrypt作為加密DNS流量的手段，所有Umbrella客戶端軟體都支援使用DNSCrypt並在預設配置中使用它。此外，自2020年2月以來，我們一直支援使用HTTPS(DoH)的DNS。

Umbrella還對傳送給上遊主管機構的查詢執行DNSSEC驗證，以確保快取中所有記錄的資料完整性。

iOS 14和macOS 11中的詳細DNS更改

iOS 14和macOS 11引入了一種選擇DNS解析器的新機制。雖然需要特定詳細資訊的客戶可以與Apple進行確認，但思科對機制的理解是可以選擇具有如下所述優先順序的DNS解析程式：

1.使用網路提供的DNS解析程式解析強制網路門戶測試區域

2. VPN或DNS代理配置（如iOS的思科安全聯結器）以及企業策略(如MDM或OTA)設定的DNS解析器。（有關設定DNS策略的詳細資訊，請諮詢您的MDM供應商）

3.由裝置所有者直接配置的系統範圍加密解析器

4.域所有者指定的加密解析程式

5.應用指定的加密解析程式

6.未加密的解析程式（如通過DHCP或RA指定的解析程式）

特別是，我們將數字3、4和5視為對解析程式選擇的重大更改，這些更改會直接影響Umbrella管理員在其網路上完全強制使用Umbrella解析程式的能力。

系統範圍的加密解析程式

使用者可以從DNS提供商安裝配置配置檔案應用，從而配置系統範圍的加密解析程式。無論網路通過DHCP或RA指定的DNS解析程式如何，此解析程式都可用於所有查詢。

目前，阻止非受管裝置使用這些解析程式的唯一已知方法是在防火牆上阻止已知DoH提供程式的IP。這樣做會導致iOS裝置的使用者發出警告，並且裝置無法回退到未加密的DNS，這意味著它無法解析DNS主機名。

由域所有者指定的加密解析程式

DNS區域的所有者可以指定用於解析其區域的特定解析程式。在iOS 14和macOS 11中，只能指定DoH解析器。此指定是使用專用的DNS記錄型別（型別65，名稱為「HTTPS」）進行的，並由DNSSEC或已知的URI進行驗證。

由於此類指定會導致查詢繞過Umbrella，因此Umbrella解析程式會針對HTTPS DNS記錄型別的查詢返回REFRESSED響應，這意味著不會發現此類指定。

應用指定的加密解析程式

如果在任何較高優先順序的機制中沒有發現其他加密解析程式，應用建立者可以指定回退加密解析程式。僅當替代方案是使用DHCP或RA設定的未加密解析程式時，才能使用此解析程式。

目前，阻止非受管裝置使用這些解析程式的唯一已知方法是在防火牆上阻止已知DoH提供程式的IP。目前尚不清楚在此類情況下，iOS是否可以回退到未加密的DNS。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。