Verstehen der Pin-Belegung und der Zertifikatsfixierung in Umbrella

Inhalt

Einleitung

In diesem Dokument werden die Zertifikatpinning und die Pin-Belegung mit öffentlichen Schlüsseln in Cisco Umbrella beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Die Zertifikatpinning ist ein Sicherheitsmechanismus im Internet, der es Anwendungen ermöglicht, Identitätswechsel mit HTTPS-Servern zu verhindern, wenn falsch ausgestellte oder anderweitig betrügerische digitale Zertifikate verwendet werden. Hierzu wird ein Server mit einem definierten Satz öffentlicher Schlüssel verknüpft, die als einzige für Verbindungen mit diesem Server vertrauenswürdig sein können. Es gibt zwei Methoden für die Zertifikatfixierung:

- Public Key Pinning (PKP RFC7469) ist ein inzwischen veralteter Mechanismus zum

Auslösen der Zertifikatpinning in Webbrowsern. Angeheftete Zertifikate werden mithilfe von HTTP-Headern an den Browser gesendet.
- Die statische Zertifikatausrichtung ist der Punkt, an dem eine Anwendung hartcodiert ist, um bestimmte Zertifikate oder Zertifizierungsstellen zu erwarten. Einige Desktop-/mobile Anwendungen verwenden einen statischen Pinning-Mechanismus für Zertifikate, um die Sicherheit zu erhöhen.

Wenn diese Webanwendungen von Umbrella als Proxy bereitgestellt werden, stimmt der von Umbrella bereitgestellte öffentliche Schlüssel nicht überein, was dazu führt, dass die Anwendung die HTTPS-Verbindung schließt. Die Zertifikatpinning gilt in der Regel nur für Desktop-/mobile Anwendungen, da die PKP-Unterstützung von modernen Webbrowsern entfernt wurde.

Kompatibilität mit Umbrella SWG

Umbrella umgeht bekannte URLs von der SSL-Entschlüsselung, um Probleme mit der Zertifikatsanheftung unter bestimmten Umständen zu beheben. Tabelle 1 enthält Anwendungen, die global für alle Umbrella-Kunden umgangen wurden. Tabelle 1 enthält auch andere Anwendungen, die zum Zeitpunkt der Dokumenterstellung bzw. beim Schreiben bekanntermaßen die Zertifikatspin-Belegung verwenden. Wenn Sie eine dieser Anwendungen verwenden, können Sie aus den angegebenen Gründen die später beschriebenen Methoden verwenden, um die Anwendung von der HTTPS-Überprüfung zu umgehen. Tabelle 2 enthält weitere Details zu den Anwendungsdiensten, die in Tabelle 1 behandelt werden.

Andere Anwendungen für das Zertifikatsanheften

Anwendungen können pro Kunde (pro Richtlinie) umgangen werden, um Probleme mit der Zertifikatpinning-Funktion mit der selektiven Entschlüsselung von Umbrella zu lösen. Diese Ausnahmen lassen sich einfach anhand der Domäne, des Anwendungsnamens oder der Kategorie implementieren. Umbrella SWG enthält eine große Bibliothek von Anwendungen in unserer App-Datenbank.

In den meisten Fällen liegt die Entscheidung, ob die Anwendung umgangen werden soll, beim IT-Administrator. Das Hinzufügen einer Entschlüsselungsausnahme ist ein Sicherheitsnachteil, da die Sicherheits-/Dateiprüfung des Webinhalts verhindert wird. Dies ist eine individuelle Entscheidung, die von der Art der Anwendung und den geschäftlichen Anforderungen abhängt. Wenn sich das Problem der Zertifikatanheftung beispielsweise nur auf eine mobile/Desktop-Anwendung auswirkt, kann der Administrator eine Ausnahme hinzufügen, um die mobile Anwendung zu aktivieren, oder stattdessen die Benutzer bitten, die Webversion der Anwendung zu verwenden.

Dies ist eine Tabelle der Anwendungen, die entweder global für Umbrella-Kunden umgangen werden, und es ist keine Aktion erforderlich oder bekannt, dass zum Zeitpunkt des Schreibens die Zertifikatpinning verwendet wird, und die nicht standardmäßig von Umbrella umgangen werden. Wenn Sie die Anwendungen verwenden, die standardmäßig nicht umgangen werden, können Sie

die oben beschriebenen Methoden aus den angegebenen Gründen verwenden, um die Anwendung von HTTPS Inspection zu umgehen.

Tabelle 1 - Anwendungen, die Zertifikatspinning verwenden können

Anwendungsname	Cisco Umbrella-Abdeckung
Adobe Services	Global umgangen für Umbrella-Kunden
Airbnb	Unterstützt durch Anwendungskontrolle
Amazon Alexa	Unterstützt durch Anwendungskontrolle
Amazon Drive	Unterstützt durch Anwendungskontrolle
Amazon Kindle	Unterstützt durch Anwendungskontrolle
Amazon-Arbeitsbereiche	Unterstützt durch Anwendungskontrolle
Amplitude	Global umgangen für Umbrella-Kunden
Anwendungsdynamik	Global umgangen für Umbrella-Kunden
Apple iMessage	Unterstützt durch Anwendungskontrolle
Apple Mail	Unterstützt durch Anwendungskontrolle
Apple Services (weitere Informationen siehe Tabelle 2)	Global umgangen für Umbrella-Kunden
Cisco Services (weitere Informationen siehe Tabelle 2)	Global umgangen für Umbrella-Kunden
Citrix Workspace	Unterstützt durch Anwendungskontrolle
Crashlytics	Global umgangen für Umbrella-Kunden

CrowdStrike Falcon	Unterstützt durch Anwendungskontrolle
Diligent.com	Unterstützt durch Anwendungskontrolle
Discord Chat	Global umgangen für Umbrella-Kunden
DocuSign-Vereinbarung - Cloud	Unterstützt durch Anwendungskontrolle
DropBox	Unterstützt durch Anwendungskontrolle
Druva Cloud-Backup	Unterstützt durch Anwendungskontrolle
Egnyte Connect	Unterstützt durch Anwendungskontrolle
Evernote	Unterstützt durch Anwendungskontrolle
Facebook-Messenger	Unterstützt durch Anwendungskontrolle
Facebook	Unterstützt durch Anwendungskontrolle
Filemail	Unterstützt durch Anwendungskontrolle
Foursquare	Unterstützt durch Anwendungskontrolle
Giphy	Global umgangen für Umbrella-Kunden
GitHub	Unterstützt durch Anwendungskontrolle
Google Drive	Unterstützt durch Anwendungskontrolle
Google Play Store	Unterstützt durch Anwendungskontrolle
Google Services (weitere Informationen siehe Tabelle 2)	Global umgangen für Umbrella-Kunden

Google-Arbeitsbereich	Unterstützt durch Anwendungskontrolle
Gehe zuMeeting	Unterstützt durch Anwendungskontrolle
Hype-Maschine	Unterstützt durch Anwendungskontrolle
Instagram	Unterstützt durch Anwendungskontrolle
LogMein Pro	Unterstützt durch Anwendungskontrolle
Microsoft Defender für Endgeräte	Unterstützt durch Anwendungskontrolle
Microsoft Intune	Unterstützt durch Anwendungskontrolle
Microsoft Services (weitere Informationen siehe Tabelle 2)	Global umgangen für Umbrella-Kunden
Microsoft Xbox Live	Unterstützt durch Anwendungskontrolle
Netflix	Unterstützt durch Anwendungskontrolle
OpenDrive	Unterstützt durch Anwendungskontrolle
PayPal	Unterstützt durch Anwendungskontrolle
PingOne-Identität	Unterstützt durch Anwendungskontrolle
Rackspace-/Cloud Drive-Services	Global umgangen für Umbrella-Kunden
Salesforce CRM	Unterstützt durch Anwendungskontrolle
Segment	Global umgangen für Umbrella-Kunden
Signal-Plattform	Unterstützt durch Anwendungskontrolle

Skype für Unternehmen	Unterstützt durch Anwendungskontrolle
Snapchat	Unterstützt durch Anwendungskontrolle
Soundcloud	Unterstützt durch Anwendungskontrolle
Spinneiche	Unterstützt durch Anwendungskontrolle
verdorben	Unterstützt durch Anwendungskontrolle
TeamViewer	Unterstützt durch Anwendungskontrolle
TikTok	Unterstützt durch Anwendungskontrolle
Todoist	Unterstützt durch Anwendungskontrolle
Twitter	Unterstützt durch Anwendungskontrolle
Vimeo	Unterstützt durch Anwendungskontrolle
Arbeitstag HCM	Unterstützt durch Anwendungskontrolle
Meetings vergrößern	Global umgangen für Umbrella-Kunden

Tabelle 2 - Details zuServices global umgangen (siehe Tabelle 1)

Apple-Services	• Captive Portal Check von Apple • Apple iTunes und App Store • Zusätzliche Apple Plattform-Services
Cisco Services	• Cisco Umbrella- und OpenDNS-Services • Cisco WebEx und WebEx Teams • Cisco Cloud Email Security - Weboberfläche • AMP-Endgerätedienst • Duo-Sicherheit 2FA

Google Services	• Google Hangouts • Google-Nachrichten im Web • Zusätzliche Google Plattform-Services
Microsoft-Services	• Microsoft-Netzwerkverbindungs-Statusanzeige • Windows-Update • Windows-Übersetzungsdienst • Zusätzliche Microsoft/Windows-Plattformdienste

Weitere Informationen finden Sie unter Problembehandlung bei Anwendungen, die nicht den Browser verwenden, oder wenden Sie sich an den Umbrella Support. Anwendungen können nach Prüfung durch das Technikerteam als Ergänzung zu unserer globalen Umgehungsliste in Betracht gezogen werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.