

Umbrella의 공개 키 피닝 및 인증서 피닝 이해

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[Umbrella SWG와의 호환성](#)

[기타 인증서 피닝 애플리케이션](#)

소개

이 문서에서는 Cisco Umbrella의 인증서 피닝 및 공개 키 피닝에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

인증서 피닝은 애플리케이션이 잘못 발급되거나 다른 방법으로 사기성 디지털 인증서를 사용하여 HTTPS 서버에 대한 가장에 저항할 수 있도록 하는 인터넷 보안 메커니즘입니다. 이는 서버를 정의된 공개 키 집합과 연결함으로써 수행됩니다. 이 공개 키는 해당 서버에 대한 연결에서만 신뢰할 수 있는 공개 키입니다. 인증서 피닝에는 두 가지 방법이 있습니다.

- PKP RFC7469(Public Key Pinning)는 이제 웹 브라우저에서 인증서 고정을 트리거하는 오래된 메커니즘입니다. 고정된 인증서는 HTTP 헤더를 사용하여 브라우저에 전송됩니다.
- 정적 인증서 피닝은 특정 인증서 또는 인증 기관을 예상하도록 응용 프로그램이 하드 코딩되는 곳입니다. 일부 데스크톱/모바일 애플리케이션에서는 보안을 강화하기 위해 고정 인증서 고정 메커니즘을 사용합니다.

이러한 웹 애플리케이션이 Umbrella에서 프록시되는 경우 Umbrella에서 제공하는 공개 키가 일치

하지 않으므로 애플리케이션이 HTTPS 연결을 닫게 됩니다. 최신 웹 브라우저에서 PKP 지원이 제거되었기 때문에 인증서 고정은 데스크톱/모바일 애플리케이션에만 가장 일반적으로 적용됩니다.

Umbrella SWG와의 호환성

Umbrella는 특정 상황에서 인증서 고정 문제를 해결하기 위해 SSL 암호 해독에서 알려진 URL을 우회합니다. 표 1에는 모든 Umbrella 고객에 대해 전역적으로 우회된 응용 프로그램이 포함됩니다. 표 1에는 작성 시 인증서 피닝을 사용하는 것으로 알려진 다른 애플리케이션도 포함되어 있습니다. 이러한 응용 프로그램을 사용하는 경우, HTTPS 검사에서 응용 프로그램을 우회하기 위해 나중에 설명하는 방법을 사용하는 것이 좋습니다. 표 2에서는 표 1에서 다루는 응용 프로그램 서비스에 대한 자세한 내용을 제공합니다.

기타 인증서 피닝 애플리케이션

Umbrella의 [선택적](#) 암호 해독 기능을 사용하여 인증서 피닝 문제를 해결하기 위해 고객별(정책별) 기준으로 애플리케이션을 [우회할](#) 수 있습니다. 이러한 예외는 도메인, 애플리케이션 이름 또는 범주에 따라 쉽게 구현할 수 있습니다. Umbrella SWG는 앱 데이터베이스에 대규모 애플리케이션 라이브러리를 포함합니다.

대부분의 경우 애플리케이션을 우회할지 여부는 IT 관리자에게 달려 있습니다. 암호 해독 예외를 추가하면 웹 콘텐츠의 보안/파일 검사를 수행할 수 없으므로 보안 경계가 해제됩니다. 이는 신청 유형 및 사업상 필요에 따라 개별적으로 결정하는 것이다. 예를 들어 인증서 피닝 문제가 모바일/데스크톱 응용 프로그램에만 영향을 미치는 경우 관리자는 모바일 응용 프로그램을 작동시키기 위해 예외를 추가하도록 선택하거나 대신 사용자에게 응용 프로그램의 웹 버전을 사용하도록 요청할 수 있습니다.

이 테이블은 Umbrella 고객을 위해 전역적으로 우회된 애플리케이션으로, 아무런 조치도 필요하지 않거나 작성 시 인증서 피닝을 사용하는 것으로 알려져 있으며 기본적으로 Umbrella에서 우회되지 않습니다. 기본적으로 우회되지 않는 애플리케이션을 사용 중인 경우 위에서 설명한 방법을 사용하여 HTTPS 검사에서 애플리케이션을 우회하는 것이 좋습니다.

표 1 - 인증서 피닝을 사용할 수 있는 애플리케이션

애플리케이션 이름	Cisco Umbrella 커버리지
어도비 서비스	Umbrella 고객을 위해 전역으로 우회
에어비앤비	애플리케이션 제어에서 지원됨
아마존 알렉사	애플리케이션 제어에서 지원됨

Amazon 드라이브	애플리케이션 제어에서 지원됨
아마존 킨들	애플리케이션 제어에서 지원됨
아마존 워크스페이스	애플리케이션 제어에서 지원됨
진폭	Umbrella 고객을 위해 전역으로 우회
앱 역학	Umbrella 고객을 위해 전역으로 우회
애플 아이메시지	애플리케이션 제어에서 지원됨
애플 메일	애플리케이션 제어에서 지원됨
Apple 서비스(자세한 내용은 표 2 참조)	Umbrella 고객을 위해 전역으로 우회
시스코 서비스(자세한 내용은 표 2 참조)	Umbrella 고객을 위해 전역으로 우회
Citrix Workspace	애플리케이션 제어에서 지원됨
파쇄학	Umbrella 고객을 위해 전역으로 우회
클라우드스트라이크 펄컨	애플리케이션 제어에서 지원됨
Diligent.com	애플리케이션 제어에서 지원됨
디스코드 채팅	Umbrella 고객을 위해 전역으로 우회
DocuSign 계약 클라우드	애플리케이션 제어에서 지원됨
드롭 박스	애플리케이션 제어에서 지원됨
Druva 클라우드 백업	애플리케이션 제어에서 지원됨
Genyte 연결	애플리케이션 제어에서 지원됨

에버노트	애플리케이션 제어에서 지원됨
Facebook 메신저	애플리케이션 제어에서 지원됨
Facebook	애플리케이션 제어에서 지원됨
파일 메일	애플리케이션 제어에서 지원됨
정사각형으로	애플리케이션 제어에서 지원됨
기피	Umbrella 고객을 위해 전역으로 우회
깃허브	애플리케이션 제어에서 지원됨
구글 드라이브	애플리케이션 제어에서 지원됨
구글 플레이 스토어	애플리케이션 제어에서 지원됨
Google 서비스(자세한 내용은 표 2 참조)	Umbrella 고객을 위해 전역으로 우회
구글 워크스페이스	애플리케이션 제어에서 지원됨
회의로 이동	애플리케이션 제어에서 지원됨
HYPE 기계	애플리케이션 제어에서 지원됨
인스타그램	애플리케이션 제어에서 지원됨
로그인 프로	애플리케이션 제어에서 지원됨
Microsoft Defender for Endpoint	애플리케이션 제어에서 지원됨
Microsoft Intune	애플리케이션 제어에서 지원됨
Microsoft 서비스(자세한 내용은 표 2 참조)	Umbrella 고객을 위해 전역으로 우회

Microsoft Xbox Live	애플리케이션 제어에서 지원됨
넷플릭스	애플리케이션 제어에서 지원됨
오픈드라이브	애플리케이션 제어에서 지원됨
페이팔	애플리케이션 제어에서 지원됨
PingOne ID	애플리케이션 제어에서 지원됨
랙 공간 / 클라우드 드라이브 서비스	Umbrella 고객을 위해 전역으로 우회
Salesforce CRM	애플리케이션 제어에서 지원됨
세그먼트	Umbrella 고객을 위해 전역으로 우회
신호 플랫폼	애플리케이션 제어에서 지원됨
비즈니스용 Skype	애플리케이션 제어에서 지원됨
스냅챗	애플리케이션 제어에서 지원됨
소리 구름	애플리케이션 제어에서 지원됨
스파이더오크	애플리케이션 제어에서 지원됨
스포티파이	애플리케이션 제어에서 지원됨
팀뷰어	애플리케이션 제어에서 지원됨
틱톡	애플리케이션 제어에서 지원됨
도도교 신자	애플리케이션 제어에서 지원됨
트위터	애플리케이션 제어에서 지원됨

비메오	애플리케이션 제어에서 지원됨
근무일 HCM	애플리케이션 제어에서 지원됨
모임 확대/축소	Umbrella 고객을 위해 전역으로 우회

표 2 - 세부 정보표 1과 같이 서비스가 전역적으로 우회됨

애플 서비스	• Apple 종속 포털 확인 • Apple iTunes 및 App Store • 추가 Apple 플랫폼 서비스
시스코 서비스	• Cisco Umbrella 및 OpenDNS 서비스 • Cisco Webex 및 Webex 팀 • Cisco Cloud Email Security WebUI • AMP 엔드포인트 서비스 • 듀오 보안 2FA
구글 서비스	• 구글 행아웃스 • 웹의 Google 메시지 • 추가 Google 플랫폼 서비스
Microsoft 서비스	• Microsoft 네트워크 연결 상태 표시기 • Windows 업데이트 • Windows 번역 서비스 • 추가 Microsoft/Windows 플랫폼 서비스

추가 도움말은 Troubleshooting Non-Browser Applications 또는 [Umbrella Support에 문의하십시오](#). 엔지니어링 팀의 검토를 거친 후 애플리케이션을 Cisco의 글로벌 바이패스 목록에 추가하는 것이 고려될 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.