

Remediate IOS-XE Security Advisory - 2026년 8월 및 관련 중요 문제

목차

소개

이 문서에서는 IOS-XE 권고 사항(2026년 8월)을 해결하기 위해 발표된 강화된 보안 릴리스와 함께 보고된 중요한 무선 소프트웨어 버그를 살펴봅니다. [Security Advisory](#), [FN74383](#) 및 [중요한](#) 문제를 [해결하는](#) 업그레이드 지침을 제공합니다.

배경

Cisco는 2026년 8월 5일 9800 series Wireless LAN Controller를 비롯한 여러 플랫폼에 영향을 주는 [IOS-XE Security Hardening Advisory](#)를 발표했습니다. 문서화된 대로, 이 권고는 Cisco IOS-XE Engineering의 포괄적인 내부 보안 검토로 인해 내부적으로 발견된 여러 취약점을 해결합니다.

검토에 포함된 무선 플랫폼

Catalyst Wireless 9800(C9800-L, C9800-CL, C9800-40, C9800-80)

Cisco Wireless 9800 WLC (CW9800L, CW9800M, CW9800H1/H2)

Embedded Wireless 9800 on Catalyst Switch(9800-SW) - SDA 구축만 지원

COS 기반 Catalyst 11ax 91xx Series Access Point(9105/9115/9117/9120/9130/9136/9164/9166)

Cisco Wireless 917x Series Access Point(CW9171/CW9172/CW9174/CW9176/CW9178/CW9179)

Cisco IOS XE 소프트웨어 릴리스	첫 번째 고정 릴리스
17.9	17.9.10
17.12	17.12.8
17.15	17.15.6

										됨
17.9.10	APSP 링크	해당 없음	APSP 링크	APSP 링크	8월 15일로 계획됨	해당 없음	해당 없음	해당 없음	APSP 링크	해당 없음

표 2. 서로 다른 9800 WLC 플랫폼에 대한 APSP 링크

CSCwv 98483

증상: C9800-L, CW9800-L, C9800-CL이 외부 WLC로 구성된 경우 IP_Learn에 고정된 무선 클라이언트 영향을 받는 플랫폼: C9800-L, CW9800-L, C9800-CL(영향을 받는 플랫폼이 외부 WLC 역할을 하는 게스트 앵커 시나리오에서만 해당)

영향을 받는 소프트웨어 버전: Cisco IOS XE 26.1.2, Cisco IOS XE 17.18.4a, Cisco IOS XE 17.15.6

해결 방법: 외부 및 앵커 간의 터널에서 모빌리티 데이터 링크 암호화를 활성화합니다.

wireless mobility group member mac-address

ip

public-ip

group

data-link-encryption

고정 릴리스: Cisco는 고정 패치/콜드 SMU를 적극적으로 사용하고 있으며, 사용 가능한 즉시 고객에게 알릴 것입니다(릴리스 예정: 8월 21일). 이는 WLC를 다시 로드해야 하는 콜드 SMU입니다.

자문 및 중요 문제에 대한 업그레이드 지침

보안이 강화된 릴리스에 대해 보고된 권고 및 중요 문제를 모두 해결하기 위해 Cisco는 다음을 권장합니다

1단계. IOS-XE 버전 17.12, 17.15, 17.18을 실행하는 무선 고객은 2, 3, 4단계로 진행합니다. IOS-XE 버전 17.9, 26.1을 실행하는 무선 고객은 업그레이드하기 전에 APSP 패치가 cisco.com에 게시될 때까지 기다립니다. 패치 릴리스 날짜는 표 2를 참조하십시오

2단계. 업그레이드 전에 [여기](#) 설명된 업그레이드 검사 및 복구 단계를 실행하여 FN으로 인한 영향을 [완화하십시오74383](#)

3단계. 보안이 강화된 IOS-XE 버전 및 APSP 패치를 동일한 유지 관리 창에서 업그레이드하여 무선 서비스가 영향을 받지 않도록 합니다.

4단계. CSCwv98483의 영향을 받는 경우 SMU를 사용할 수 있을 때까지 해결 방법을 적용합니다. SMU가 게시되면 고객은 SMU 패치를 적용할 것으로 예상됩니다.

IOS-XE 업그레이드 + 패치 유지 관리 기간 계획을 위한 다운타임 고려 사항

비이중화 또는 고가용성(HA) 이중화 구성으로 구성된 9800 WLC의 IOS-XE 업그레이드는 다음과 같은 다양한 메커니즘을 활용할 수 있습니다

- ISSU(서비스 중 소프트웨어 업그레이드)
- N+1 롤링 업그레이드
- 1회성 업그레이드

자세한 내용은 [9800 WLC 업그레이드 빠른 시작 가이드를 참조하십시오](#)

또한 SMU(Software Maintenance Update) 및 APSP(Access Point Service Pack)를 사용하여 패치를 적용해야 하는 중요한 문제가 있습니다

9800 WLC에서 지원하는 다양한 패치 옵션에 대한 자세한 내용은 9800 WLC용 [패치 및 롤링 AP 업그레이드 가이드를 참조하십시오](#)

각 업그레이드 메커니즘을 통한 IOS-XE 업그레이드 + 패칭을 위한 유지 관리 기간을 계획하려면 이 섹션에 설명된 다운타임 및 영향을 고려하십시오.

ISSU(서비스 중 소프트웨어 업그레이드)

- HA SSO(Stateful Switchover) 컨피그레이션에서 실행되는 9800 WLC 쌍에만 적용되며 장기 릴리스 트레인과 해당 유지 보수 릴리스 간에만 지원됩니다. (유지 보수 릴리스가 없는 에스컬레이션 릴리스 및 단기간 릴리스 열차에서 지원되지 않음)
- ISSU는 HA SSO에서 9800 쌍을 지원하면서 다양한 소프트웨어 버전을 실행하고 롤링 AP 업그레이드를 활용하여 원활한 업그레이드 환경을 제공합니다. 작동 중인 9800 HA 쌍에서 대기 WLC가 업그레이드되고 SSO 후 새 대기 WLC가 업그레이드됩니다. ISSU 프로세스 및 해당 CLI 및 GUI 스냅샷에 대한 자세한 내용은 ISSU를 [사용하여 9800 HA SSO 업그레이드를](#)

참조하십시오

- ISSU를 시작하기 전에 AP에서 업그레이드 확인 및 복구를 실행합니다.
- ISSU에서는 구축 규모 및 네트워크 속도에 따라 WLC 및 모든 AP에서 보안이 강화된 IOS-XE 이미지를 활성화할 최대 시간이 정의되지 않으며 대규모 구축에서는 "몇 시간"으로 실행될 수 있습니다.
- 또한 ISSU는 AP가 지연 방식으로 리부팅되는 롤링 AP 업그레이드를 활용하여 다운타임을 최소화합니다. 그러나 이 경우 강화된 릴리스를 실행하는 AP에 연결된 클라이언트에서는 ISSU 업그레이드 후 WLC에 패치를 적용할 때까지 CSCwv93265 및 CSCwv98483에 [설명된](#) 연결 및 로밍 문제가 계속 발생합니다.
- CSCwv98483용 [SMU](#)는 WLC 다시 로드가 필요한 콜드 패치입니다.
- CSCwv93265용 [APSP](#)는 롤링 AP 업그레이드를 사용하여 또는 원샷으로 적용할 수 있습니다. 롤링 AP 업그레이드를 사용하는 경우 구축 규모에 따라 모든 AP가 업그레이드되는 데 몇 "시간"이 소요될 수 있으며 알려진 심각한 버그를 확실히 방지할 수 있습니다
- 서비스가 영향을 받을 수 있는 총 기간(WLC 또는 AP가 다운되었거나 클라이언트 연결/로밍이 영향을 받음) = ISSU 완료 시간 + SMU 콜드 패치로 인한 WLC 다시 로드 시간 + APSP의 AP 롤링 업그레이드 시간

N+1 롤링 AP 업그레이드

- 이 절차에서는 호스트 AP에 대해 소프트웨어 버전이 업그레이드된 N+1 WLC라고 하는 예비 품 9800 WLC를 사용하지만 "프로덕션" 9800 쌍 또는 9800 독립형 업그레이드는 진행합니다. N+1 롤링 업그레이드를 시작하기 전에 이 N+1 9800 WLC에 AP가 등록되지 않는 것이 좋습니다.
- AP가 기본 WLC에 등록된 상태에서 업그레이드 검사 및 복구를 실행합니다.
- 프로세스 및 관련 CLI 및 GUI 스냅샷에 대한 자세한 내용은 [N+1 롤링 AP 업그레이드를 사용하여 9800 WLC 업그레이드를 참조하십시오](#)
- 이 프로세스에서 AP가 기본 WLC에서 N+1 WLC로 원활하게 롤오버하려면 N+1 WLC에서 실행되고 AP에 사전 다운로드된 소프트웨어 버전이 정확히 일치해야 합니다.
- 기본 WLC에서 IOS-XE 강화 릴리스를 다운로드하면 AP에 대한 사전 다운로드가 진행되지만 활성화하지는 않습니다. 이미지를 활성화하지 않으면 소프트웨어 패치를 AP에 적용하거나 미리 다운로드할 수 없습니다. 이는 N+1 WLC도 패치할 수 없음을 의미합니다.
- 이 프로세스에서도 ISSU와 같이 N+1 WLC로 롤오버된 AP는 롤링 AP 업그레이드가 완료된 후 N+1 WLC에 패치를 적용할 때까지 CSCwv93265 및 CSCwv98483에 설명된 클라이언트 연결 및 로밍 문제의 위험이 계속 있습니다.
- CSCwv98483용 [SMU](#)는 WLC 다시 로드가 필요한 콜드 패치입니다.
- CSCwv93265용 [APSP](#)는 롤링 AP 업그레이드를 사용하여 또는 원샷으로 적용할 수 있습니다. 롤링 AP 업그레이드를 사용하는 경우 구축 규모에 따라 모든 AP가 업그레이드되는 데 몇 "시간"이 소요될 수 있으며 알려진 심각한 버그를 확실히 방지할 수 있습니다
- 서비스가 영향을 받을 수 있는 총 기간(WLC 또는 AP가 다운되었거나 클라이언트 연결/로밍이 영향을 받음) = 모든 AP가 N+1 WLC로 롤오버하는 데 걸린 시간 + SMU 콜드 패치로 인한 WLC 다시 로드 시간 + APSP에 대한 AP 롤링 업그레이드 시간
- 유지 보수 기간에서 N+1 WLC를 IOS-XE 강화 릴리스로 업그레이드하고 AP가 기본 WLC에서 IOS-XE 강화 릴리스를 사전 다운로드하는 데 걸리는 시간도 고려하지만, 이 두 가지 모두 서비스에 영향을 미치지 않습니다

N+1 일반 AP 업그레이드 - 권장

- 이 절차에서는 "프로덕션" 9800 쌍 또는 9800 독립 실행형 독립 실행형 업그레이드가 진행되는 동안 호스트 AP에 업그레이드된 소프트웨어 버전이 있는 N+1 WLC로 예비품 9800 WLC 케이블을 사용합니다.
- N+1 롤링 업그레이드가 시작되기 전에 이 예비품 9800 WLC에 등록된 AP가 없는 것이 좋습니다.
- 예비 N+1 WLC를 업그레이드하여 강화 IOS-XE를 활성화 및 커밋하고 APSP 및 SMU로 한 번에 패치할 수 있습니다. 등록된 AP가 없는 경우 이는 비서비스 영향이지만 유지 보수 기간을 예약할 때 여러 WLC 다시 로드 소요되는 시간을 고려해야 합니다
- AP가 등록된 기본 WLC GUI에서 COnfiguration(컨피그레이션) > Tags and Profiles(태그 및 프로파일)로 이동합니다. AP 프라임 > 기본
 - N+1 WLC 및 WMI(Wireless Management Interface) IP 주소를 기본으로 정의
 - 보조에서 현재 기본 WLC 이름 및 WMI IP 정의
- regex 필터를 사용하여 기본 WLC에서 N+1 WLC로 AP를 대량 마이그레이션합니다.
- N+1 WLC에 등록되면 AP는 중요 버그를 해결하기 위한 패치와 함께 보안 강화 릴리스를 이미 실행하고 있습니다.

서비스가 영향을 받을 수 있는 총 기간(WLC 또는 AP가 중단되거나 클라이언트 연결/로밍이 영향을 받음) = AP가 기본 WLC에서 N+1 WLC로 마이그레이션하는 데 걸리는 시간(AP와 WLC 간의 네트워크 속도에 따라 결정됨)

1회 업그레이드 - N+1 WLC가 없는 경우 권장

- 이 절차에서는 기본 WLC를 활성화 및 약속과 함께 보안 강화 IOS-XE 릴리스로 한 번에 업그레이드합니다.
- 이미지 활성화의 일환으로 기본 WLC가 다시 로드되고 모든 AP가 업그레이드 기본 WLC에 다시 등록되며 보안이 강화된 IOS-XE 릴리스를 수신합니다.
- APSP가 적용될 때까지 AP는 CSCwv93265 및 CSCwv에 설명된 클라이언트 연결 및 로밍 [문제](#)에 [노출될 수 있습니다98483](#)

서비스가 영향을 받을 수 있는 총 기간(WLC 또는 AP가 다운되거나 클라이언트 연결/로밍이 영향을 받음) = 기본 WLC가 다시 로드하는 데 걸린 시간 + 모든 AP가 CAPWAP를 통해 기본 WLC에서 강화된 IOS-XE 릴리스를 다운로드하고 기본 WLC에 다시 등록하는 데 걸린 시간(SMU 패치가 적용되는 경우 이 시간을 두 배) + 모든 AP가 기본 WLC에서 APSP 패치를 다운로드하고 기본 WLC에 다시 등록하는 데 걸린 시간

자주 묻는 질문(FAQ)

Q1. AP가 이 보안 권고의 영향을 받습니까?

COS 기반 액세스 포인트는 보안 검토에 포함되었으며 해당 수정 사항은 강화된 IOS-XE 릴리스에 통합되었습니다

Q2. AireOS WLC의 위험은 무엇입니까?

AireOS WLC는 LDoS(Last Day of Support)에 도달했으므로 보안 검토에 포함되지 않았습니다.

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.