# 2016년 9월 28일 반기별 Cisco IOS 및 IOS XE Software Security Advisory 번들 게시 요약

'+'Top of the section'+''); } function endA() { //alert("end"); document.write('

'); } function startExpandoIndentSubheader() { document.write('
'); } function endExpandoIndentSubheader() { document.write('
'); } function endIndent() { //alert("end"); document.write('

'+''+''+'+'[Expand all sections]'+' '+' [Collapse all sections]'+'+''+''+'+'Close Section'+'

**자문 ID:cisco-sa-20160928-번들**

http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20160928-bundle

## 개정 1.0

**2016년 9월 28일 16:00 UTC(GMT)**

---

## 목차



---

## 요약


2016년 9월 28일 릴리스된 Cisco IOS 및 IOS XE Software Security Advisory 번들 발행물에는 Cisco IOS 및 IOS XE Software의 11개 취약성을 설명하는 10개의 Cisco 보안 권고 사항이 포함되어 있습니다.전체 권고 사항 목록 및 관련 링크는 Cisco 이벤트 응답: 2016년 9월 Cisco IOS 및 IOS XE Software Security Advisory 번들 게시.


## 소프트웨어 버전 및 수정 사항

Cisco는 이 번들 발행물에 설명된 취약성을 해결하는 무료 소프트웨어 업데이트를 발표했습니다.

## 고정 소프트웨어 가져오기

Cisco는 이 번들 발행물에 설명된 취약성을 해결하는 무료 소프트웨어 업데이트를 발표했습니다.고객은 라이센스를 구매한 소프트웨어 버전 및 기능 세트에 대해서만 지원을 설치하고 요청할 수 있습니다.이러한 소프트웨어 업그레이드를 설치, 다운로드, 액세스 또는 기타 방법으로 사용함으로써 고객은 Cisco 소프트웨어 라이센스 약관에 동의하는 것입니다.
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

또한 고객은 유효한 라이센스를 보유하고 있거나 Cisco에서 직접 조달하거나 Cisco 공인 리셀러 또는 파트너를 통해서만 소프트웨어를 다운로드할 수 있습니다.대부분의 경우 이전에 구매한 소프트웨어로 유지 보수 업그레이드가 이루어집니다.무료 보안 소프트웨어 업데이트를 통해 고객은 새 소프트웨어 라이센스, 추가 소프트웨어 기능 집합 또는 주요 수정 버전 업그레이드를 받을 수 없습니다.

소프트웨어 업그레이드를 고려할 때, 고객은 Cisco Security Advisories and Alerts 페이지에서 제공하는 Cisco 제품의 권장 사항을 정기적으로 참조하여 위험과 완벽한 업그레이드 솔루션을 확인하는 것이 좋습니다.

모든 경우, 고객은 업그레이드할 디바이스에 충분한 메모리가 포함되어 있는지 확인하고 새 릴리스에서 현재 하드웨어 및 소프트웨어 컨피그레이션이 계속 제대로 지원되는지 확인해야 합니다.정보가 명확하지 않은 경우, 고객은 Cisco TAC(Technical Assistance Center) 또는 계약된 유지 관리 공급업체에 문의하는 것이 좋습니다.

## 서비스 계약이 있는 고객

계약을 보유한 고객은 정기적인 업데이트 채널을 통해 소프트웨어를 얻어야 합니다.대부분의 고객은 Cisco.com의 Software Center를 통해 소프트웨어 패치 및 버그 수정을 받아야 합니다.

## 타사 지원 조직을 사용하는 고객

Cisco 파트너, 공인 리셀러 또는 서비스 제공자와 같은 타사 지원 조직과의 이전 또는 기존 계약을 통해 Cisco 제품을 제공 또는 유지 관리하는 고객은 해당 지원 조직에 연락하여 이 조언과 관련하여 적절한 행동 방침을 안내하고 지원해야 합니다.

해결 방법 또는 픽스의 효과는 제품 혼합, 네트워크 토폴로지, 트래픽 동작, 조직 임무 등 특정 고객 상황에 따라 달라집니다.다양한 영향을 받는 제품 및 릴리스로 인해 고객은 서비스 제공업체 또는 지원 조직과 협의하여 적용된 해결 방법 또는 수정 사항이 구축되기 전에 의도한 네트워크에서 사용하는 것이 가장 적절한지 확인해야 합니다.

## 서비스 계약이 없는 고객

Cisco에서 직접 구매하지만 Cisco 서비스 계약을 보유하고 있지 않은 고객과 타사 벤더를 통해 구매하지만 POS(point-of-sale)를 통해 고정 소프트웨어를 구매하지 못한 고객은 Cisco TAC(Technical Assistance Center)에 문의하여 업그레이드를 받아야 합니다.
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

고객은 제품 일련 번호를 사용할 수 있어야 하며 무료 업그레이드를 받을 수 있는 자격 증명으로 본 조언의 URL을 제공할 준비가 되어 있어야 합니다.

# 이 공지의 상태:최종

이 문서는 "있는 그대로" 제공되며 상품성 또는 특정 용도에 대한 적합성에 대한 보증을 포함하여 어떠한 종류의 보증이나 보증도 의미하지 않습니다.문서 또는 문서에서 링크된 자료에 대한 정보를 사용하는 것은 사용자의 책임입니다.CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

다음 섹션에서 배포 URL을 생략하는 이 문서의 텍스트를 독립형 사본이나 패러프레이즈는 제어되지 않는 사본이며 중요한 정보가 없거나 사실 오류를 포함할 수 있습니다.이 문서의 정보는 Cisco 제품의 최종 사용자를 위한 것입니다.

## 배포

이 알림은 다음 링크에서 사용할 수 있습니다.
http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20160928-bundle

또한 이 알림의 텍스트 버전은 Cisco PSIRT(Product Security Incident Response Team) PGP 키로 명확하게 서명되어 다음 이메일 및 사용자 뉴스 수신자에게 전송됩니다.

- bugtraq@securityfocus.com
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco@newsgate.cisco.com
- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- full-disclosure@lists.grok.org.uk
- vulnwatch@vulnwatch.org

이 알림의 향후 업데이트(있는 경우)는 Cisco.com에 게시되지만 메일 목록이나 뉴스 그룹에 적극적으로 알리거나 그렇지 않을 수도 있습니다.고객은 위의 URL에서 이 알림의 업데이트를 확인하는 것이 좋습니다.

## 개정 기록

## Cisco 보안 절차

Cisco 제품의 보안 취약성 보고, 보안 사고에 대한 지원을 받고, Cisco로부터 보안 정보를 받기 위해 등록하는 방법에 대한 자세한 내용은 Cisco 보안 취약성 정책을 참조하십시오.또한 이 정책에는 Cisco 보안 취약성 정보와 관련된 홍보 관련 연락처 정보 및 언론 문의가 포함됩니다.

모든 Cisco Security Advisories는 http://www.cisco.com/go/psirt에서 확인할 수 있습니다.