

Summary of the 반기별 Cisco IOS and IOS XE Software Security Advisory Bundled Publication, 2017년 3월 22일

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

'); } function startExpandIndentSubheader() { document.write('

'); } function endExpandIndentSubheader() { document.write('

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

'+'+'+'+'[\[Expand all sections\]](#)'+' '+'[\[Collapse all sections\]](#)'+'+'+'[Close Section](#)'+'

자문 ID:cisco-sa-20170322-번들

<https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20170322-bundle>

개정 1.0

2017년 3월 22일 16:00 UTC(GMT) 공개 릴리스

목차

[요약](#)

[소프트웨어 버전 및 수정 사항](#)

[고정 소프트웨어 가져오기](#)

[이 공지문의 상태:최종](#)

[배포](#)

[개정 기록](#)

[Cisco 보안 절차](#)

요약

이 문서는 2017년 3월 22일 Cisco IOS 및 IOS XE Software Security Advisory 번들 발행물 릴리스에 포함되어 있으며 5개의 취약성을 설명하는 5개의 Cisco 보안 권고 사항이 포함되어 있습니다. .Advisories의 전체 목록 및 링크를 보려면 [Cisco Event Response:2017년 3월 Cisco IOS 및 IOS XE Software Security Advisory 번들 게시](#).

[소프트웨어 버전 및 수정 사항](#)

소프트웨어 업그레이드를 고려할 때, 고객은 [Cisco Security Advisories and Alerts 페이지](#)에서 제공

하는 Cisco 제품의 권장 사항을 정기적으로 참조하여 위험과 완벽한 업그레이드 솔루션을 확인하는 것이 좋습니다.

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

고정 소프트웨어 가져오기

Cisco는 권장 사항에 설명된 취약성을 해결하는 소프트웨어 업데이트를 릴리스했습니다. 고객은 라이선스를 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 라이선스 약관에 동의하는 것입니다.

<http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN.html>

또한 고객은 유효한 라이선스를 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 라이선스, 추가 소프트웨어 기능 집합 또는 주요 수정 버전 업그레이드를 받을 수 없습니다.

소프트웨어 업그레이드에 대해서는 psirt@cisco.com 또는 security-alert@cisco.com에 문의하지 마십시오.

서비스 계약이 있는 고객

계약을 보유한 고객은 정기적인 업데이트 채널을 통해 소프트웨어를 얻어야 합니다. 대부분의 고객은 Cisco 전 세계 웹 사이트(<http://www.cisco.com>)의 Software Center를 통해 소프트웨어를 업그레이드해야 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 권고와 관련된 적절한 조치 과정에 대한 안내 및 지원을 받아야 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 이 문서의 URL을 무료 업그레이드 자격 증명으로 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.

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 문서는 Cisco 전 세계 웹 사이트()에 게시되어 있습니다.

<https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20170322-bundle>

이 문서의 텍스트 버전은 전 세계 웹 게시뿐만 아니라 Cisco PSIRT PGP 키로 서명되어 다음 이메일 및 사용자 뉴스 수신자에게 게시됩니다.

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

이 문서의 향후 업데이트(있는 경우)는 Cisco 전 세계 웹 사이트에 게시되지만 메일 목록 또는 뉴스 그룹에 적극적으로 알려거나 그렇지 않을 수도 있습니다. 이 문제를 우려하는 사용자는 이전 URL에서 모든 업데이트를 확인하는 것이 좋습니다.

개정 기록

Cisco 보안 절차

Cisco 제품의 보안 취약점 보고, 보안 사고 지원, Cisco로부터 보안 정보를 받기 위한 등록 등에 대한 자세한 내용은 Cisco 전 세계 웹 사이트(<http://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html>)을 [참조하십시오](#). 여기에는 Cisco 보안 취약성 정보와 관련된 언론 문의 지침이 포함됩니다. 모든 Cisco Security Advisories는 <http://www.cisco.com/go/psirt>에서 [확인할](#) 수 있습니다.