2019년 9월 25일 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-20190925-번들

https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20190925-bundle

개정 1.0

2019년 9월 25일 15시 30분 UTC(GMT)

목차

요약

Cisco는 2019년 9월 25일 반기별 Cisco IOS 및 IOS XE Software Security Advisory 번들 발행물을 발표했습니다.고객 피드백에 대한 직접적인 응답으로 Cisco는 Cisco IOS 및 IOS XE Software Security Advisories 번들을 매년 3월과 9월에 4번째 수요일에 릴리스합니다.

2019년 9월 25일 릴리스된 Cisco IOS 및 IOS XE Software Security Advisory 번들 발행물에는 Cisco IOS Software 및 Cisco IOS XE Software의 13가지 취약성을 설명하는 12개의 Cisco 보안 권고 사항이 포함되어 있습니다.Cisco는 이러한 취약성을 해결하는 소프트웨어 업데이트를 발표했습니다.

모든 취약성은 SIR(Security Impact Rating)가 높음취약성을 성공적으로 악용하면 공격자가 무단 액세스 권한을 얻거나, 명령 주입 공격을 수행하거나, 영향을 받는 디바이스에서 DoS(서비스 거부) 조건을 발생시킬 수 있습니다.

두 가지 취약성은 Cisco IOS Software 및 Cisco IOS XE Software에 모두 영향을 미칩니다.두 가지

취약성이 Cisco IOS Software에 영향을 미치며, 8개의 취약성이 Cisco IOS XE Software에 영향을 미칩니다.취약성 중 하나는 Cisco IOx 애플리케이션 환경에 영향을 미칩니다.Cisco는 어떤 취약점도 Cisco IOS XR Software 또는 Cisco NX-OS Software에 영향을 미치지 않는다고 확인했습니다.

특정 Cisco IOS 또는 IOS XE Software 릴리스가 하나 이상의 취약성의 영향을 받는지 신속하게 확인하려면 Cisco IOS 소프트웨어 검사기를 사용합니다.

소프트웨어 버전 및 수정 사항

소프트웨어 업그레이드를 고려할 때는 http://www.cisco.com/go/psirt 및 후속 권고 사항을 참조하여 노출을 확인하고 완벽한 업그레이드 솔루션을 확인하십시오.

모든 경우, 업그레이드 대상 장치에 충분한 메모리가 포함되어 있는지, 새 릴리스에서 현재 하드웨어 및 소프트웨어 컨피그레이션이 계속 제대로 지원되는지 확인하도록 주의해야 합니다.정보가 명확하지 않은 경우 Cisco TAC(Technical Assistance Center) 또는 계약 유지 보수 공급업체에 문의하십시오.

고정 소프트웨어 가져오기

Cisco는 이러한 취약성을 해결하는 소프트웨어 업데이트를 발표했습니다.소프트웨어를 배포하기 전에 고객은 유지 관리 공급업체에 문의하거나 해당 환경에 대한 기능 집합 호환성 및 알려진 문제가 있는지 소프트웨어를 확인해야 합니다.

고객은 구매한 기능 세트만 설치하고 지원을 받을 수 있습니다.이러한 소프트웨어 업그레이드를 설치, 다운로드, 액세스 또는 다른 방법으로 사용함으로써 고객은 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html에 있는 Cisco의 소프트웨어 라이센스 약관 또는 Cisco.com Downloads(http://www.cisco.com/public/sw-center/sw-usingswc.shtml)에 명시된 바로 동의하게 됩니다.

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 고객에게 소프트웨어 패치 및 버그 픽스는 Cisco의 전 세계 웹 사이트(http://www.cisco.com)의 Software Center를 통해 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

Cisco로부터 직접 구매하지만 Cisco 서비스 계약을 보유하고 있지 않은 고객과 타사 벤더를 통해 구매하지만 POS를 통해 고정 소프트웨어를 구매하지 못한 고객은 Cisco TAC(Technical Assistance Center)에 문의하여 소프트웨어 패치 및 버그 수정을 받아야 합니다.TAC 연락처는 다음과 같습니다.

- +1 800 553 2447(북미 지역 무료 전화)
- +1 408 526 7209(전 세계 어디에서나 유료 전화)
- email:tac@cisco.com

고객은 제품 일련 번호를 사용할 수 있어야 하며, 소프트웨어 패치 또는 버그 픽스를 받을 수 있는 자격 증명으로 이 알림 URL을 제공할 준비가 되어 있어야 합니다.서비스 계약이 없는 고객은 TAC을 통해 소프트웨어 패치 또는 버그 수정을 요청해야 합니다.

현지화된 전화 번호, 지침 및 다양한 언어로 사용할 이메일 주소 등 추가 TAC 연락처 정보는 http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html를 참조하십시오.

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 본 문서의 독립형 사본 또는 패러프레이즈는 통제되지 않은 사본이며 중요한 정보가 없거나 사실 오류를 포함할 수 있습니다.

배포

이 조언은 Cisco의 전 세계 웹 사이트()에 게시되어 있습니다.

https://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20190925-bundle

이 알림의 텍스트 버전은 전 세계 웹 게시뿐만 아니라 Cisco PSIRT PGP 키로 명확하게 서명되어

다음 이메일 및 사용자 뉴스 수신자에게 게시됩니다.

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- fulldisclosure@seclists.org
- comp.dcom.sys.cisco@newsgate.cisco.com

이 조언의 향후 업데이트(있는 경우)는 Cisco의 전 세계 웹 사이트에 게시되지만 메일링 목록 또는 뉴스 그룹에 적극적으로 알리거나 그렇지 않을 수도 있습니다.이 문제를 우려하는 사용자는 위의 URL에서 업데이트를 확인하는 것이 좋습니다.

개정 기록

처음 게시됨:2019년 9월 25일

상태:최종

버전:1.0

Cisco 보안 절차

Cisco 제품의 보안 취약점 보고, 보안 사고 지원, Cisco로부터 보안 정보를 받기 위한 등록 등에 대한 자세한 내용은 Cisco의 전 세계 웹 사이트 (http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html)을 참조하십시오 .여기에는 Cisco 보안 알림에 대한 언론 문의 지침이 포함됩니다.모든 Cisco 보안 권고 사항은 http://www.cisco.com/go/psirt에서 확인할 수 있습니다.