보안 참조 정보

Security Advisories and Notices(보안 권고 및 알림)는 http://www.cisco.com/go/psirt에 있으며 PSIRT(Product Security Incident Response Team)의 추가 정보도 함께 제공됩니다.

모범 사례

Cisco 라우터의 보안 개선

이 문서에서는 네트워크 관리자가 보안을 개선하기 위해 라우터에서 특히 경계 라우터에서 변경해야 하는 몇 가지 Cisco 구성 설정에 대해 비공식적으로 설명합니다.이 문서는 IP 네트워크에서 거의 보편적으로 적용할 수 있는 기본적인 "공통" 구성 항목에 대한 것이며, 몇 가지 예상치 못한 항목에 대해 알아두어야 합니다.

Cisco IOS 비밀번호 암호화 팩트

Cisco가 아닌 소스가 Cisco 구성 파일에서 사용자 비밀번호(및 기타 비밀번호)를 해독하는 프로그램을 릴리스했습니다.프로그램은 enable secret 명령으로 설정된 비밀번호**를 해독하지** 않습니다.이 프로그램이 Cisco 고객 사이에서 야기된 예기치 않은 문제로 인해 많은 고객이 Cisco 비밀번호 암호화에 의존하여 제공한 것보다 더 많은 보안을 실현하고 있는 것으로 의심되었습니다.이 문서에서는 Cisco 비밀번호 암호화의 보안 모델 및 해당 암호화의 보안 제한에 대해 설명합니다.

Cisco의 SAFE 청사진

SAFE는 조직이 e-비즈니스를 안전하게 수행할 수 있도록 하는 포괄적인 보안 청사진입니다 .SAFE는 네트워크의 성장과 변화에 따라 보안 설계, 배포 및 관리를 간소화하는 모듈형 접근 방식을 사용하여 Cisco AVVID(Architecture for Voice, Video and Integrated Data)에 구축된 네트워크를 개선합니다.

공격 방어, 추적 또는 완화 전략

Cisco 라우터를 사용한 패킷 플러드 특성 및 추적

> DoS(서비스 거부) 공격은 인터넷에서 흔히 발생합니다.이러한 공격에 대응하는 첫 번째 단계는 정확히 어떤 종류의 공격인지 파악하는 것입니다.일반적으로 사용되는 대부분의 DoS 공격은 고대역폭 패킷 플러드 또는 기타 반복적인 패킷 스트림을 기반으로 합니다.이 문서에서는 이러한 공격을 이해하고 추적하는 방법에 대한 통찰력을 제공합니다.

닙다 바이러스 퇴치 전략

이 인덱스는 Nimda Virus를 처리하기 위한 모든 기술 팁 및 완화 권장 사항의 포괄적인 목록을 제공합니다.

코드 레드 지렁이 퇴치 전략

이 인덱스는 코드 레드(Code Red) WORM을 처리하기 위한 모든 기술 팁 및 완화 권장 사항의 포괄적인 목록을 제공합니다.

DDoS(Distributed Denial of Service) 공격으로부터 보호하기 위한 전략

이 백서에서는 잠재적인 DDoS 공격이 어떻게 발생하는지에 대한 기술적 설명과 Cisco IOS Software를 사용하여 이를 방어하는 방법을 제시합니다.

UDP 진단 포트 서비스 거부 공격으로부터 보호하기 위한 전략

이 백서에서는 잠재적인 UDP 진단 포트 공격 발생 방식에 대한 기술 설명과 Cisco IOS 소프트웨어를 사용하여 이를 방어하는 방법을 제시합니다.

TCP SYN 서비스 거부 공격으로부터 보호하기 위한 전략

이 백서에서는 잠재적인 TCP SYN 공격이 발생하는 방법에 대한 기술 설명과 Cisco IOS 소프트웨어를 사용하여 이를 방어하는 방법을 제시합니다.

서비스 거부 공격의 최신:"스머페팅" 설명 및 정보를 통한 효과 최소화

참고:위 링크는 Cisco Systems, Inc.에서 유지 관리하지 않는 외부 사이트를 가리킵니다.

Cisco 라우터에 중점을 두고 이러한 공격의 영향을 줄이는 방법을 통해 "smurf" 공격에 대한 자세한 정보를 제공합니다.일부 정보는 일반적으로 조직의 특정 공급업체와 관련되지 않으며,그러나 Cisco 라우터에 중점을 두고 작성되었습니다.이 문서는 "스머프" 공격이 다른 공급업체의 장비에 미치는 영향을 확인하는 내용이 아닙니다.그러나 다양한 벤더에 대한 정보가 포함되어 있습니다.

기타 리소스

Cisco 제품 보안 사고 대응

이 문서에서는 버그 보고 및 사고 대응 절차에 대해 설명합니다. 특히, 현재 보안 공격이 진행 중이거나 공격이 있을 경우, Cisco 제품에 보안 문제가 있을 경우, Cisco 제품에 대한 기술 보안 정보를 얻고자 하거나, Cisco 제품에 대해 발표된 보안 문제에 대해 추가 질문이 있을 경우,보안 사고를 처리하는 Cisco PSIRT(Product Security Incident Response Team)의 역할에 대해 설명합니다.
