

보안 취약점 자료

문서 제목	Cisco WSA 제품 취약점 보안 업데이트 권고
문서 번호	A3AEGIS-20170724-001
작성 일자	2017년 07월 24일
제공 부서	에이쓰리 침해대응센터

보안 취약점 자료

제 목	Cisco WSA 제품 취약점 보안 업데이트 권고
내 용	<ul style="list-style-type: none"><input type="checkbox"/> 개요<ul style="list-style-type: none">o Cisco社は 자사의 제품에 영향을 주는 취약점을 해결한 보안 업데이트 발표 [1]o 공격자는 해당 취약점을 악용하여 원격 코드 실행, 권한 상승 등의 피해를 발생시킬 수 있으므로 최신 버전으로 업데이트 권고 <input type="checkbox"/> 설명<ul style="list-style-type: none">o Cisco Web Security Appliance(WSA)의 웹 인터페이스에서 사용자 입력 값 검증 미흡으로 권한 상승 및 원격 코드 실행이 가능한 취약점(CVE-2017-6746) <input type="checkbox"/> 해당 시스템<ul style="list-style-type: none">o 영향을 받는 제품<ul style="list-style-type: none">- 참고사이트에 명시되어 있는 'Affected Products'을 통해 취약한 제품 확인 <input type="checkbox"/> 해결 방안<ul style="list-style-type: none">o 취약점이 발생한 Cisco 소프트웨어가 설치된 이용자는, 해당되는 참고사이트에 명시되어 있는 'Affected Products' 내용을 확인하여, 패치 적용 <p>[참고사이트]</p> <p>[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-wsa1</p>