Cisco 제품군 취약점 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.21

□ 개요
o Cisco社는 자사 제품의 취약점을 해결한 보안 업데이트 공지
o 공격자는 해당 취약점을 이용하여 임의 명령어 실행 등의 피해를 발생시킬 수 있으므로, 해당 제품을 사용하는 이용자들은 최신 버전으로 업데이트 할 것을 권고

□ 주요 내용
o Cisco Prime Infrastructure에서 SSL 인증서에 대한 검증이 미흡하여 발생하는 정보노출 취약점(CVE-2019-1659) [1]
o Cisco Prime Collaboration Assurance(PCA) Software에서 인증 기능이 미흡하여 발생하는 권한상승 취약점(CVE-2019-1662) [2]
o Cisco Network Convergence System 1000 Series의 software에서 사용자의 입력값에 대한 검증이 미흡하여 발생하는 정보노출 취약점(CVE-2019-1681) [3]
o Cisco HyperFlex Software에서 입력값 검증 및 인증 기능이 미흡하여 발생하는 명령어 삽입 취약점(CVE-2018-15380, CVE-2019-1664) [4][5]

□ 영향을 받는 제품
o Cisco Prime Infrastructure Software
 - 3.5 이전 버전
o Cisco Prime Collaboration Assurance(PCA) Software
 - 12.1 SP2 이전 버전
o Cisco Network Convergence System 1000 Series(IOS XR Software)
 - 6.5.2 이전 버전
o Cisco HyperFlex Software
 - 3.5(2a) 이전 버전

□ 해결 방안
o 취약점이 발생한 Cisco 제품 이용자는 참고사이트에 명시되어 있는 'Fixed Software' 내용을 확인하여 패치 적용

□ 기타 문의사항
o 한국인터넷진흥원 인터넷침해대응센터: 국번없이 118

[참고사이트]
[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-prime-validation
[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-pca-access
[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-ncss
[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-hyperflex-injection
[5] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-chn-root-access

주소 : 서울특별시 서초구 서초대로 255 고덕빌딩 2층 [06595]
전화 : 02-2105-4400 (영업문의 1, 보안관제문의 2, 기술문의 3)
팩스 : 02-2105-4456
영업문의 : sales@eosec.co.kr, 보안관제 및 기술문의 : tech@eosec.co.kr
COPYRIGHTS © 아이온시큐리티 ALL RIGHTS RESERVED.