Cisco 제품군 취약점 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.03.18

□ 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 Common Services Platform Collector(CSPC)에서 기본 PW 사용으로 인해 임의의 원격사용자가 관리자 권한으로 로그인할 수 있는 권한 상승 취약점(CVE-2019-1723) [1]

o Open Container Initiative runc CLI tool을 사용중인 Cisco 제품에서 파일 서술자(file descriptor)에 대한 처리가 미흡하여 발생하는 권한상승 취약점(CVE-2019-5736) [2]

□ 영향을 받는 제품

o Cisco Common Services Platform Collector(CSPC)

- 2.7.2 ~ 2.7.4.5 버전
- 2.8.x ~ 2.8.1.2 이전 버전

o Cisco의 Open Container Initiative tool 관련 제품

- Container Platform
- Cloudlock
- Defense Orchestrator

□ 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-20190313-cspcscv

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190215-runc

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