리눅스 snapd 취약점(dirty sock) 보안 업데이트 권고

출처 : 인터넷침해대응센터
작성일 : 2019.02.18

□ 개요
o 리눅스의 snap 데몬에서 권한상승 취약점(dirty sock)을 해결한 보안 업데이트 발표 [1]
o 악용코드가 공개되어 있으므로 영향 받는 버전을 사용 중인 이용자는 해결방안에 따라 적극적인 업데이트 필요
※ snap 패키지 : 소프트웨어 설치 및 제거를 쉽게 사용할 수 있도록 사용자 편의를 지원하는 서비스 패키지

□ 설명
o snapd API에서 UNIX 소켓에 대한 접근 통제가 미흡하여, 공격자가 해당 API에 접근하여 관리자 권한을 탈취할 수 있는 권한상승 취약점(CVE-2019-7304)

□ 영향 받는 제품
o snap API : 2.28 ~ 2.37 버전
- 버전 확인 방법 : 커맨드 창에서 “snap version” 입력
※ 우분투 리눅스의 경우 snap 데몬이 기본으로 설치가 되어있으므로, 영향받는 버전을 사용 중인 경우 반드시 업데이트 필요

□ 해결 방안
o 제조사 홈페이지를 참고하여 최신버전으로 보안 업데이트 수행 [2]
- 2.37.1 이상 버전으로 업데이트

□ 기타 문의사항
o 한국인터넷진흥원 인터넷침해대응센터: 국번없이 118

[참고사이트]
[1] https://people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-7304.html
[2] https://forum.snapcraft.io/t/installing-snapd/6735

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.