Lookin Enterprise Use Case

상세 조치 가이드로 취약점 셀프 개선

IT시스템 분야별 전문 운영 인력을 보유하지 않은 기업도 Lookin Enterprise가 제공하는 명령어 수준의 상세 조치 가이드를 활용하여 외부 전문가의 도움 없이 고객 스스로 손쉽게 취약점을 개선할 수 있습니다.

점검기준

정상 : 점검기준에 맞게 설정됨
취약 : 점검기준에 맞게 설정되지 않음

*점검기준

1. 아래와 같이 TCP SACK 버그 패치 중 하나라도 설치된 경우
11.23 : PHNE_42094, PHNE_43215
11.31 : PHNE_42470, PHNE_43412, PHNE_43814, PHNE_44266
2. #/usr/bin/ndd -get /dev/tcp tcp_sack_enable ==> 0

* PHNE_44547(16/11/29) for 11.31 설치되어 있으면, 대체패치가 설치된 것으로 문제 해결됨(문제번호 QXCR1001454218)

점검 결과

TCP SACK 관련 버그 패치가 설치되어 있음
11.23 : PHNE_42094, PHNE_43215
11.31 : PHNE_42470, PHNE_43412, PHNE_43814, PHNE_44266

취약시 문제점

TCP SACK 관련 패치 문제로 인해 네트워크로 전송된 데이터가 corruption 될 수 있음

조치 가이드

아래와 같이 설정
1) tcp tcp_sack_enable 0 설정
2) nddconf 파일에도 적용
3) ndd명령으로 설정 enable

[참조]

*설정 방법

1) NDD 파라미터 수정(online 수정 - 신규 세션부터 적용됨)
/usr/bin/ndd -set /dev/tcp tcp_sack_enable 0
2) nddconf 파일에도 적용(리부팅 후에도 적용됨)
/etc/rc.config.d/nddconf
TRANSPORT_NAME[x]=tcp
NDD_NAME[x]=tcp_sack_enable
NDD_VALUE[x]= 0

- 보고서 수준의 상세 진단 결과 리포트
- 지표화 된 진단결과로 개선 목표 관리 용이
- 명령어 수준의 상세 조치 가이드 제공