Handling Kernel Security Problems

https://lwn.net/Articles/290227/

2076122 류성경

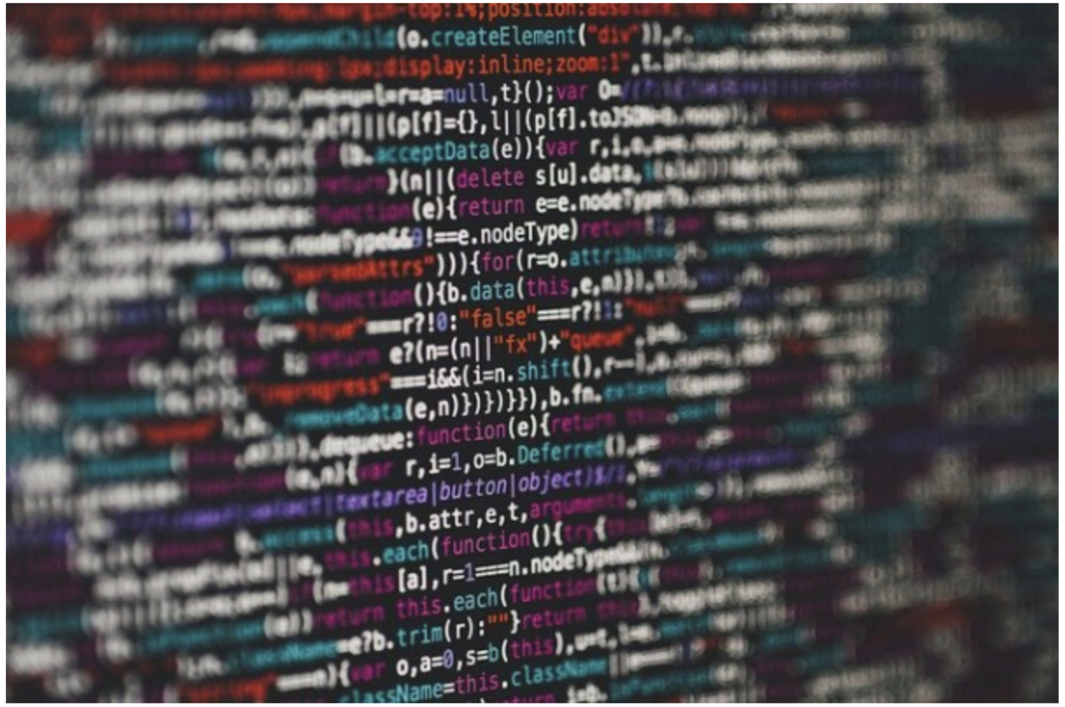
리눅스 커널이란?

- Linux OS의 주요 구성 요소로, 컴퓨터 하드웨어와 프로세스를 잇는 핵심 인터페이스

출처: https://www.dailysecu.com/news/articleView.html?idxno=121925

리눅스 커널에서 15년 된 심각한 보안취약점 발견돼

길민권 기자 | 승인 2021.03.14 15:29



사용자는 어떻게 하면
보안문제로부터 안전할 수 있을까?

리눅스 재단은 자사의 커널에서 발생하는 보안취약점에 대한 보안 업데이트를 발표했다.

공격자는 취약점을 악용해 피해를 발생시킬 수 있으므로, 영향받는 제품을 이용 중인 사용자는 최신버전으로 보안 업데이트를 적용해야 안전할 수 있다.

올해 초 발표한 보안 업데이트

사용자는 어떻게 하면 보안문제로부터 안전할 수 있을까?

2.3. Linux

계정 관리(5개 항목), 파일 및 디렉토리 관리(14개 항목), 서비스 관리(15개 항목), 패치 및 로그 관리(2개 항목) 총 4개 영역에서 36개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 계정 관리	U-01	root 계정 원격 접속 제한	상
	U-02	패스워드 복잡성 설정	상
	U-03	계정 잠금 임계값 설정	상
	U-04	패스워드 최대 사용 기간 설정	중
	U-05	패스워드 파일 보호	상
나. 파일 및 디렉토리 관리	U-06	root 홈, 패스 디렉터리 권한 및 패스 설정	상
	U-07	파일 및 디렉터리 소유자 설정	상
	U-08	/etc/passwd 파일 소유자 및 권한 설정	상
	U-09	/etc/shadow 파일 소유자 및 권한 설정	상
	U-10	/etc/hosts 파일 소유자 및 권한 설정	상
	U-11	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상
	U-12	/etc/syslog.conf 파일 소유자 및 권한 설정	상
	U-13	/etc/services 파일 소유자 및 권한 설정	상
	U-14	SUID, SGID, Sticky bit 설정 파일 점검	상
	U-15	사용자 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상
	U-16	world writable 파일 점검	상
	U-17	$HOME/.rhosts, hosts.equiv 사용 금지	상
	U-18	접속 IP 및 포트 제한	상
	U-19	cron 파일 소유자 및 권한 설정	상
다. 서비스 관리	U-20	Finger 서비스 비활성화	상
	U-21	Anonymous FTP 비활성화	상
	U-22	r 계열 서비스 비활성화	상
	U-23	DoS 공격에 취약한 서비스 비활성화	상
	U-24	NFS 서비스 비활성화	상
	U-25	NFS 접근통제	상
	U-26	automountd 제거	상
	U-27	RPC 서비스 확인	상
	U-28	NIS, NIS+ 점검	상
	U-29	tftp, talk 서비스 비활성화	상
	U-30	Sendmail 버전 점검	상
	U-31	스팸 메일 릴레이 제한	상
	U-32	일반사용자의 Sendmail 실행 방지	상
	U-33	DNS 보안 버전 패치	상
	U-34	DNS ZoneTransfer 설정	상
라. 패치 및 로그관리	U-35	최신 보안패치 및 벤더 권고사항 적용	상
	U-36	로그의 정기적 검토 및 보고	상

[표 3] Linux서버 진단 체크리스트

'한국인터넷진흥원'에서 발표한 <클라우드 취약점 점검 가이드>
출처 : https://isms.kisa.or.kr/main/csap/notice/?boardId=bbs_0000000000000004&mode=view&cntId=45

사용자는 어떻게 하면
보안문제로부터 안전할 수 있을까?

가. 계정 관리

진단항목	U-01. root 계정 원격 접속 제한	취약도	상
항목설명	각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 통해 root 원격 접속 차단이 적용되지 않은 시스템의 root 계정 정보를 비인가자가 획득할 경우 시스템 계정 정보 유출, 파일 및 디렉터리 변조 등의 행위 침해사고가 발생할 수 있다.		
진단기준	양호	원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우	
	취약	원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우	
진단방법	▪ Telnet 1) /etc/securetty 파일에 pts/0 ~ pts/x 관련 설정이 존재하는지 확인 # cat /etc/securetty ※ tty(terminal-teletype) : 서버와 연결된 모니터, 키보드 등을 통해 사용자가 콘솔로 직접 로그인함 ※ pts(pseudo-terminal, 가상터미널) : Telnet, SSH, 터미널 등을 이용하여 접속함 ▪ SSH 1) /etc/ssh/sshd_config 파일에서 Root 로그인 설정 확인 # cat /etc/ssh/sshd_config | grep PermitRootLogin		

```
[root@localhost ~]# cat /etc/securetty | grep pts
[root@localhost ~]# cat /etc/securetty | grep tty
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS0
ttysclp0
3270/tty1
```


보안상 위험이 있는 부분을
사전에 점검하고,
안내된 진단 및 해결 방법에 따라
보안 문제를 대비할 수 있음.

감사합니다.