

PC-04 (상)	2. 서비스 관리 > 2.2 불필요한 서비스 제거
취약점 개요	
점검내용	<ul style="list-style-type: none"> ■ 사용하지 않는 서비스나 디폴트로 설치되고 있는 서비스가 있는지 점검
점검목적	<ul style="list-style-type: none"> ■ 사용하지 않는 서비스나 디폴트로 설치된 서비스들을 제거하여 시스템 자원의 낭비를 막고 해당 서비스 포트를 통한 침입을 방지
보안위협	<ul style="list-style-type: none"> ■ 실질적으로 사용하지 않는 서비스들이 실행되어 시스템에 과부하가 발생함 ■ 불필요한 서비스의 경우 사용자가 알지도 못한 서비스들이 실행되고 있는 경우가 대부분, 이 경우 해당 서비스가 이미 취약한 버전의 서비스인지도 인지하지 못하고 사용함
참고	<ul style="list-style-type: none"> ■ 불필요한 서비스가 시스템에 디폴트로 설치되어 실행되는 경우 시스템 자원을 낭비하게 될 뿐만 아니라, 이 서비스를 통해 악의적인 공격자가 침입할 수 있으므로 필요하지 않은 서비스는 중지시켜야 함 ■ 시스템 관리자는 대상 시스템의 용도를 정확히 파악한 후 특별한 목적으로 사용하는 업무관련 서비스를 제외한 다른 불필요한 서비스를 제거하여야 함 <p>※ OS 버전에 따라 '일반적으로 불필요한 서비스' 목록에 나열된 서비스가 제공되지 않을 수 있음</p>
점검대상 및 판단기준	
대상	<ul style="list-style-type: none"> ■ Windows XP, Windows 7, Windos 8.1, Windows 10
판단기준	<p>취약 : 일반적으로 불필요한 서비스(아래 목록 참조)가 구동 중인 경우</p>

조치방법	불필요한 서비스 중지	
	서비스명	기능 및 설명
	Alerter	네트워크상에서 사용자와 컴퓨터에 관리용 경고 메시지를 전송하는 기능
	Automatic Updates	중요한 윈도우 업데이트를 다운로드하고 설치할 수 있도록 하는 애플리케이션. 수동패치를 적용하거나, MS패치 관리 서버로 패치를 일괄적으로 관리하는 경우 불필요한 서비스
	Clipbook	서버 내 Clipbook을 다른 클라이언트와 공유
	Computer Browser	네트워크에 있는 모든 컴퓨터의 목록을 업데이트하고 관리하는 기능
	Cryptographic Services	윈도우 파일의 서명을 확인하는 카탈로그 데이터베이스 서비스를 총괄
	DHCP Client	IP 주소와 DNS 이름을 DHCP 서버에 등록하거나 DHCP 서버로부터 동적으로 IP주소를 가져오는 기능을 수행. 단독으로 시스템을 수행하며 고정IP를 사용하는 경우 불필요한 서비스
	Distributed Link Tracking Client, Server	네트워크 도메인의 여러 컴퓨터나 일반컴퓨터에서 NTFS 파일간의 연결을 관리하는 도구. Active Directory가 구성되어 있지 않은 서버에서는 불필요한 서비스
	DNS Client	컴퓨터에 대한 도메인 이름 시스템(DNS)이름을 확인하고 캐시에 보관하는 기능. DNS서버가 아닌 시스템에서는 유명무실하나, IPSEC을 사용하는 경우 필요한 경우 있음
	Error reporting Service	프로그램 오류가 발생 시 응용프로그램의 오류를 MS에 보고한다는 내용을 표시하는 기능
	Human Interface Device Access	키보드 또는 기타 멀티미디어 장치에 사전 정의된 버튼들을 사용하는 HID장치들을 위한 서비스
	IMAPI CD-Burning COM Service	서버에 CD-RW 또는 DVD-RW가 장착되어 보조 백업장치 역할을 하기 위해서 자체 레코딩 백업을 할 수 있음
	Infrared Monitor	사용자 적외선 연결을 통해 파일 및 이미지를 공유할 수 있도록 함

	Messenger	클라이언트와 서버 사이에 netsend 및 경고서비스 메시지를 전송하는 기능
	NetMeeting Remote Desktop Sharing	윈도우9X 운영체제부터 인증된 사용자가 넷미팅을 사용해서 원격으로 컴퓨터에 접근할 수 있도록 하는 기능
	Portable Media Serial Number	컴퓨터에 연결된 이동성 음악연주기(미디기기)의 등록번호를 복원하는 기능
	Print Spooler	인쇄 과정에 있는 스푼링을 관리하는 서비스. 프린터가 있는 경우 필수 서비스이나, 프린터가 연결되지 않은 시스템에서는 불필요함
	Remote Registry	원격 사용자가 이 컴퓨터에서 레지스트리 설정을 수정할 수 있도록 설정하는 애플리케이션
	Simple TCP/IP Services	Echo, Discard, Character Generator, Daytime, Quote of the Day 지원
	Universal Plug and Play Device Host	네트워크 장치에 대해 피어-투-피어 UPnP(범용 플러그 앤 플레이) 기능을 지원
	Wireless Zero Configuration	802.11 어댑터에 대해 자동 구성을 공급하는 기본적인 도구
조치 시 영향	일반적인 경우 영향 없음	