

웹변조 예방위해 환경설정 변경하세요

사용하지 않는 설치관련 파일은 삭제하고 패치 적용
최근 수일 해킹으로 국내 2,300여 웹사이트변조 피해

한국정보보호진흥원(KISA, 원장 이홍섭)은 최근 대규모 웹변조 피해가 잇따르는 가운데 무료로 배포되어 활용되는 웹사이트 게시판 프로그램의 취약점이 발견되고 있어 웹사이트 관리자 및 사용자의 주의를 당부했다.

웹사이트 변조를 방지하려면 웹서버 및 게시판 구동 프로그램을 최신 버전으로 업그레이드하고 환경설정 보안을 강화하여야 한다.

또한 게시판 프로그램의 일종인 코웹로그(KorWeblog)의 취약점이 공개되었지만 공식패치가 발표되지 않아 이로 인한 웹변조 피해를 막기 위해서는 사용하지 않는 설치관련 파일 삭제, 환경설정 파일의 수정 및 패치를 적용해야 한다.

※ 코웹로그(KorWeblog) : 사용자가 원하는 대로 수정할 수 있는 PHP 기반의 게시판, 자료실, 사용자등록, 접속 통계, 로그기록 등을 관리할 수 있는 공개용 무료 콘텐츠 관리 프로그램

KISA는 취약점 발견시 인터넷침해사고대응지원센터(전화번호 02-118, <http://www.krcert.or.kr>)로 신속히 신고해 줄 것을 당부했다.

한편 지난 12월 28일부터 1월 4일까지 국내에서는 2,300여 웹사이트가

변조되는 피해가 발생했다. 이처럼 단기간에 많은 피해가 발생한 것은 피해 웹사이트들이 동일한 구성 및 프로그램을 활용하여 내용만 다르게 구성하는 가상 호스팅(virtual hosting) 웹사이트이어서 피해가 더욱 확산되었기 때문이다.

해커그룹은 동일한 취약점을 악용하여 유사한 방식으로 다량의 웹사이트를 변조시킨 것으로 분석되었다. 해커그룹은 피해를 입은 가상 웹사이트들이 웹사이트 보안을 위한 필수 설정사항인 웹 주소를 통한 파일열기 금지설정 (allow_url_fopen = Off)을 하지 않았음을 파악하고 원격에서 프로그램을 웹사이트에 삽입하여 실행(PHP injection), 대량으로 웹사이트를 변조했다.

※ 웹변조 방지를 위한 조치사항(KrCERT 홈페이지참조 : <http://www.krcert.or.kr>)

- PHP 최신 프로그램(PHP 4.3.10 및 PHP 5.0.3) 업그레이드
(<http://www.php.net/downloads.php>)
- php.ini 환경설정 파일 내용을 다음과 같이 수정
 - allow_url_fopen의 값을 'on'에서 'off'로 수정
- 제로보드 최신버전(4.1 pl5) 업그레이드
(http://www.nzeo.com/bbs/zboard.php?id=main_notice&no=176)
- 그누보드 최신버전(3.40) 업그레이드
(http://sir.co.kr/?doc=bbs/gnuboard.php&bo_table=pds&page=1&wr_id=1871)
- phpBB 최신버전(2.0.11) 업그레이드
(<http://www.phpbb.com/downloads.php>)
- **코웹로그** 취약점 해결방안
 - php.ini 파일의 magic_quotes_gpc의 기본값인 'on' 유지
(http://kldp.net/tracker/index.php?func=detail&aid=300654&group_id=13&atid=300013)
- **테크노트** 취약점 해결방안
 - Lib-5.cgi 및 print.cgi에 소스 수정
(<http://www.technote.co.kr/cgi-sys/cgiwrap/cgiour/techttop/technote2/read.cgi?board=notice>)