

개인정보위, PHP 보안 취약점 관련 개인정보 유출 예방조치 당부

- PHP 보안 패치 및 DB 관리도구 접근통제 등 긴급 보호조치 안내
- 개인정보 대량조회, 반출 등 의심스러운 접속 점검 등 관리 체계 강화

개인정보보호위원회(위원장 송경희, 이하 ‘개인정보위’)는 최근 공개된 PHP 보안 취약점과 관련하여 공공기관과 민간기업 등 개인정보처리자에게 개인정보 유출 예방을 위한 보호조치를 당부했다.

지난 10월 21일 발표된 ‘PHP2Shell’은 공격자가 별도의 로그인이나 인증 절차 없이도 웹서버에서 임의의 악성 명령을 실행할 수 있는 취약점으로, 과기정통부와 한국인터넷진흥원이 이번 취약점에 대한 조치 방안을 안내하였다.

※ 한국인터넷진흥원 보호나라(boho.or.kr) → 알림마당 → 보안공지 → 「PHP 제품 보안 업데이트 권고」 참고

PHP는 웹서비스 개발·운영에 널리 사용되는 소프트웨어로, 취약점이 악용될 경우 웹 서버 침해뿐 아니라 연계된 데이터베이스(DB)에 저장된 이용자의 개인정보 유출로 이어질 우려도 있다.

특히, PHP 기반의 DB 관리도구인 phpMyAdmin 등이 외부에 노출되어 있거나 과도한 DB 접근권한이 부여된 경우, 공격자가 이를 악용해 대량의 개인정보에 접근할 위험이 있어 각별한 주의가 필요하다.

이에 개인정보위는 웹 서비스를 운영하는 개인정보처리자에게 다음과 같은 보호조치를 신속히 이행할 것을 당부했다.

- ① **(취약점 긴급 조치)** PHP 사용 시스템의 버전을 확인하고, 최신 보안패치를 적용하는 한편 불필요한 웹서비스를 삭제
- ② **(DB 접근통제 강화)** phpMyAdmin 등 DB 관리도구의 인터넷 직접 접근을 제한하고, phpMyAdmin 소프트웨어의 버전을 확인해 업데이트 하고 불필요한 설정파일 등 정리. 특히, 웹서비스 계정의 개인정보 DB 접근권한을 최소화
- ③ **(대량유출 방지)** 개인정보 DB의 대량조회·반출 등 비정상 접근 여부를 점검하고, 이상 행위 탐지·차단 및 접속기록 관리 강화
- ④ **(관리 사각지대 점검)** 외주 개발·운영 시스템, 수탁업체 및 호스팅환경 에서 사용 중인 PHP 소프트웨어 등은 없는지 확인하고 조치

양청삼 개인정보위 사무처장은 “이번 취약점은 홈페이지 자체의 침해에 그치지 않고, 이와 연결된 데이터베이스에 저장된 다수 이용자의 개인정보가 유출되는 등 대규모 피해로 이어질 우려가 있다”라며, “보안 업데이트와 함께 의심스러운 접속 점검 등 관리 체계를 강화하여 국민의 개인정보가 유출되지 않도록 각별히 주의해야 한다”라고 말했다.

담당 부서	예방조정심의관	책임자	과 장	김해숙 (02-2100-3060)
	사전실태점검과	담당자	사무관	전이루 (02-2100-2448)

