IT Chosun

"뽐뿌 해킹사고, 허술한 웹 취약점 관리가 발단"

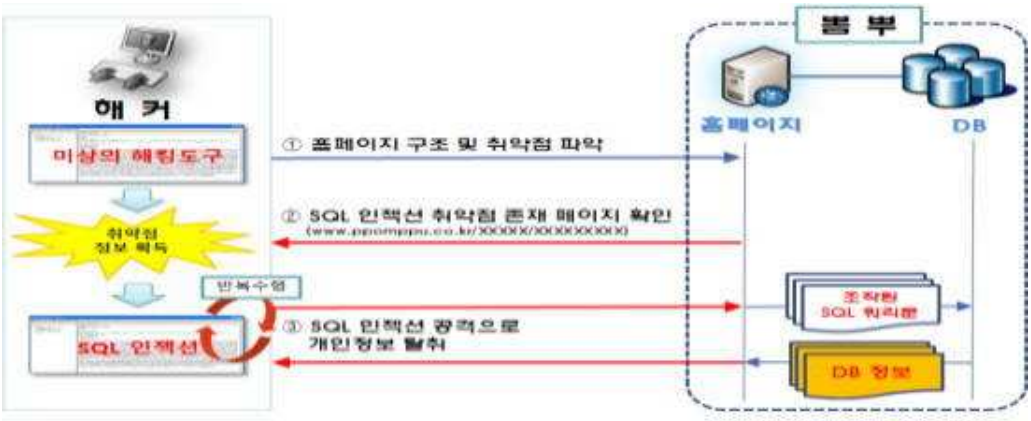
기사입력 2015.10.20 14:28:07 | 최종수정 2015.10.20 14:28:07 | 노동균 기자 | yesno@it.co.kr

[IT조선 노동균] 지난 9월 11일 온라인 커뮤니티 '뽐뿌' 해킹사고는 웹 취약점을 악용한 데이터베이스(DB) 공격이 발단이었던 것으로 나타났다.

미래창조과학부는 20일 약 196만 명의 회원정보를 유출한 뽐뿌 홈페이지 침해사고와 관련해 해킹 방법, 사고 원인 등에 대한 민·관 합동조사단의 조사 결과를 발표했다.

조사단은 해킹 방법과 정보 탈취에 악용된 보안취약점 확인을 위해 뽐뿌에 남아있는 약 10만 건의 웹 서버 로그와 약 2890만 건의 개인정보 DB 등을 분석했다. 그 결과, 해커는 뽐뿌 홈페이지 구조 및 취약점을 파악하고, SQL 인젝션에 취약한 웹 페이지를 확인한 후 SQL 인젝션을 통해 개인정보를 탈취한 것으로 드러났다.

SQL 인젝션이란 DB에 대한 질의값인 SQL 구문을 조작해 정상적인 자료 이외에 해커가 원하는 자료까지 DB로부터 유출 가능한 공격 기법을 말한다.



조사단에 따르면, 해킹 당시 뽐뿌 홈페이지에는 비정상적인 DB 질의에 대한 검증절차가 없어 SQL 인젝션 공격에 취약한 웹페이지가 존재했다. 당초 해당 웹페이지는 숫자만을 입력받는 역할을 해야 하나, 정상적인 숫자 외에 ID, 생년월일, 이메일 등 개인정보를 질의하는 SQL 구문 삽입 및 실행이 가능한 상태였던 것.

이에 조사단은 추가적인 해킹 피해 방지를 위해 뽐뿌 홈페이지에 대한 취약점 점검, 디도스(DDoS) 사이버대피소 적용 등의 긴급 기술지원을 실시했다고 설명했다.

아울러 유사 피해를 방지하기 위해 커뮤니티 관련 업체에 취약점 점검 및 보안조치를 하도록 요청하는 한편, 향후 사이버공격에 신속히 대응하기 위해 방통위, 경찰 등 관계기관과 긴밀히 협력해 나갈 계획이라고 밝혔다.

노동균 기자 **yesno@chosunbiz.com**

노동균 기자 (yesno@it.co.kr)

창닫기