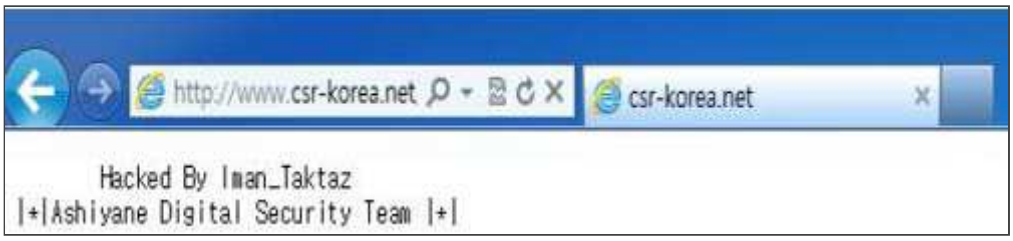
보안뉴스 미디어

대한상의 '지속가능경영포털' 해외 해커 침입...보안 취약

2013-10-10

해커침입 흔적과 함께 디렉토리 리스팅·파일업로드 취약점 발견!
지속가능경영포털 "시스템 점검 통해 적절한 보안강화 조치 취할 것"

[보안뉴스 김태형] 대한상공회의소 지속가능경영원에서 운영하고 있는 '지속가능경영포털 사이트(www.csr-korea.net)'가 해외 해커에 의해 침입 당한 흔적과 함께 디렉터리 리스팅 취약점과 파일 업로드 취약점이 발견됐다.



▲ 지속가능경영포탈 사이트의 해외 해커 침입 흔적.

이러한 취약점을 발견한 보안전문가 김관영 씨는 "대한상공회의소가 운영하는 지속가능경영포털 사이트가 지난 9월에 해외 해커에게 침입 당한 흔적을 발견했다. 이는 공격자들이 자신을 과시하기 위해서 침입한 후, 흔적을 남긴 것으로 보인다"라고 밝혔다.

이어서 그는 "디렉토리 리스팅 취약점은 브라우저에서 URL 입력란에 파일명 이하를 삭제하고 바로 디렉토리에 접근을 시도했을 경우, 에러 화면이 뜨지 않고 디렉 토리의 하위 내용이 보여지면 디렉토리 리스팅 취약점이 존재하는 것"이라고 설명했다.

▲ 디렉토리 내부의 모든 파일이 보여지는 디렉토리 리스팅 취약점.

이 취약점은 디렉토리는 물론, 내부의 모든 파일들이 보이게 되어 공격자는 웹 어플리케이션의 구조를 파악해 민감한 정보가 포함된 설정 파일을 조회하거나 웹에 게시하지 않은 각종 파일을 유출할 수 있다.

이와 함께 발견된 파일 업로드(File Upload) 취약점은 애플리케이션 개발·운영 환경과 동일한 언어로 작성된 공격 파일을 웹 서버 측에 업로드 한 후, 원격으로 해당 파일에 접근해 실

행시키는 취약점이다.

이 취약점은 작성된 공격 파일의 기능에 따라서 위험도가 다양해져 공격자가 조작한 'Server Side Script' 파일을 업로드하고 업로드 된 파일이 서버 상에 저장된 경로를 유추한 후, 이 경로를 통해 'Server Side Script' 파일을 실행하면 일종의 Shell을 획득할 수 있고 이러한 과정을 통해 웹 서버의 권한이 노출될 수 있어 위험하다.

김관영 씨는 "지속가능경영포털 사이트의 디렉토리 리스팅 취약점은 웹서버 관리 미흡으로 발생하는 취약점으로 공격자는 이를 통해 웹 애플리케이션의 구조를 파악하고 민감한 데이터를 조회하거나 추가적인 공격방법을 구상할 수 있다"면서 "이에 대응하기 위해서는 웹상에서 디렉터리 검색을 차단해야 한다"라고 밝혔다.

또한 그는 "파일 업로드 취약점의 경우, Server Side Script 파일에 대한 검증 부족으로 인해 발생하는 취약점으로 공격자는 이를 이용해 웹셸을 업로드하고 시스템을 장악할 수 있다"면서 "이 사이트에 웹셸 업로드 시 정상적으로 웹셸이 실행되는 것을 알 수 있었다. 공격자가 웹 서버에 이러한 웹셸을 심어 놓은 후 한참 뒤에 이를 작동시켜 스팸메일 발송이나 개인정보 유출 등과 같은 명령을 실행시킬 수 있다"라고 설명했다.

김관영 씨는 "이러한 취약점에 대응하기 위해서는 업로드를 처리하는 웹 소스코드에서 첨부파일의 확장자를 보고 필터링하거나 디렉터리 스크립트 실행 설정을 제거해서 웹셸이 업로드 되더라도 실행하지 않게 환경을 설정해야 한다"고 강조했다.

이와 관련 지속가능경영포털 웹사이트 관계자는 "해외 해커의 침입 흔적은 지난 9월 하순경에 발견해 조치를 취했고 디렉토리 리스팅 취약점과 파일 업로드 취약점에 대해서는 현재 점검을 통해 적절한 보안강화 조치를 취할 것"이라고 말했다.
[김태형 기자(boan@boannews.com)]