보안침해방지를 위한 취약성 점검 조치 안내

2018. 01. 17 미분류

-보안침해방지를 위한 취약성 점검 조치 안내-

최근 발생한 보안침해사고에 대한 분석결과와 조치에 대하여 안내 드립니다.

지난 해 12월경, 영림원소프트랩 내 외부개발자용 서버의 해킹으로 인해 해당 웹사이트의 업데이트 모듈이 변조되어, 악성코드 유포지로 접속을 유도하는 보안침해사고가 발생하였습니다.
분석 결과, 해당 서버의 파일업로드 취약점을 이용한 웹쉘 생성으로 웹사이트 경로 내 업데이트 모듈이 변조되었습니다.
이로 인해 2017년 12월 19일부터 12월 27일 17시까지 해당 웹사이트에 접속한 기기가 2차 악성코드에 감염된 것으로 파악되었습니다.

– 침해 사이트 : devout.ksystem.co.kr
– 파일업로드 취약점 : WebFileUpload.aspx
– 변조된 업데이트 모듈 : ClientUpdater.exe (2017년 6월 22일자 파일이며 디지털서명 없음)
– 2차 악성코드 : AngKor.exe

이에 따라 영림원소프트랩은 정부기관과 협력하여 침해서버의 보안취약점을 제거하고 변조된 업데이트 모듈을 다운로드 한 기기를 모두 확인하여 악성코드제거, OS재설치 등 모든 조치를 완료하였습니다.
또한 파일업로드 취약점이 있는 고객을 대상으로 악성코드 감염여부를 전수 검사하였습니다.
검사결과, 침해사이트로부터 업데이트 모듈이 다운로드 된 기기외에는 악성코드가 발견되지 않아 추가 피해는 없었습니다.

앞으로 영림원소프트랩은 보안침해사고가 발생되지 않도록 다음과 같이 재발방지에 노력하겠습니다.
– 설치 및 패치 프로그램 보안 강화
– 시스템 보안인프라 강화(침입탐지, 변조, 악성코드유포 등에 초기대응)
– 패치 프로그램 무결성 보장을 위한 기능 추가 등

문의처: se@ksystem.co.kr

Share:

Share your thoughts

댓글 *

[redacted]

이름 *

이메일 *

웹사이트

다음 번 댓글 작성을 위해 이 브라우저에 이름, 이메일, 그리고 웹사이트를 저장합니다.

Comment