데일리시큐

뉴스 이슈

[데일리시큐 TV] XML 해킹공격, PC정보 유출 이렇게 이루어져!

기업보안담당자, XML 파서 설정 안전하게 변경해 운영해야!

장성협 shjang@dailysecu.com 2013년 08월 28일 수요일

여름 휴가를 마치고 돌아온 이주원 대리(31세. 가명)는 가족과 여행지에서 함께 찍은 사진과 동영상파일이 외부 사이트에 노출된 것을 발견했다.

평소 PC는 백신 등 보안은 꼼꼼이 챙겼다고 자부했지만 자신의 PC 정보가 유출돼 크게 당황한 것이다. 이대리는 평소 친분이 있는 보안전문가인 지인에게 자초지종을 설명한 결과 뜻밖의 이야기를 들었다.

유출된 경로를 추적한 결과 기존에 잘 알려지지 않은 XML 공격을 통해 정보 유출이 이루어진 것을 알게 된 것이다. 데일리시큐는 보안전문가와 함께 이 공격에 대해 자세히 알아보는 시간을 가지고 그 내용을 영상으로 담았다.

[데일리시큐 TV] XML 공격기법

<영상 우측 하단 전체화면 클릭. 풀HD화면으로 선명한 영상을 볼 수 있다>

XML 공격기법의 경우 오래전부터 OWASP를 비롯해 알려진지 오래됐다. 하지만 한정된 진

단 기간과 정보 유출과 관련된 해킹기법이 SQL 인젝션, 파일업로드 등 체크리스트 항목에 한정된 허점을 파고들며 다시 해커들의 주요 공격 기법이 된 것이다.

진단 시, XML 공격에 대해 보안인들 조차 의외로 인지하지 못하는 사람들이 많다고 한다. 공격기법이 동작하면 XML 웹서비스가 되는 서버에 디렉토리 경로와 파일명을 알 수가 있다. 이를 통해 웹서비스 디렉토리 아래 개인 파일이 존재하면 웹브라우저를 통해 다운을 받을 수 있는 것이다.

이 취약점이 동작하는 이유는 XML 파서(번역기)가 취약하게 설정돼 서버의 디렉토리와 파일정보를 공격자에 노출하게되어 발생하는 것이다. 따라서 이공격을 해결하기 위해 기업 보안 관리자는 XML 파서 설정을 안전하게 변경하여 운영할 필요가 있다.

이에 데일리시큐에서는 이상훈 타이거팀 팀장을 만나 이 공격기법이 어떻게 이뤄지는지 영상으로 진행하게 됐다.

한편 사용된 일부 기술 내용은 OWASP에서 발췌한 것을 사전에 알린다.

XML은 표준 문서 형식으로 단말기(PC, 모바일 등)에서 웹서버의 웹서비스와 통신할 때 사용되는 형식중 하나이다.

-참고자료 및 대응방법 : OWASP 2013 “XML Attack Surface”, Pierre Ernst ,
www.slideshare.net/OWASP_Ottawa/pierre-ernst-xml-attack-surface-owasp-ottawa

영상취재=데일리시큐 장성협 기자 shjang@dailysecu.com

장성협의 다른 기사보기