시티즌랩 연구진, 한국의 청소년 유해정보 차단 앱에서 중요한 보안 및 프라이버시 문제점 발견

September 20, 2015

Tagged: Asia Chats, Smart Sheriff, South Korea

Categories: Press Releases

Read the press release in English.

즉시 배포용
캐나다 토론토: 2015년 9월 20일

오늘 토론토 대학교 뭉크스쿨 글로벌상황연구소 산하 시티즌랩 (Munk School of Global Affairs, Citizen Lab)에서는 새로운 보고서 "우리의 아이들은 안전한가? 청소년들을 디지털 위험에 노출시키는 한국의 스마트보안관 앱(Are the Kids Alright? Digital Risks to Minors from South Korea's Smart Sheriff Application)"을 발표한다. 동 보고서는 한국 정부가 권장하는 유해정보 차단 소프트웨어인 "스마트보안관"의 프라이버시 보호 정도 및 보안성에 대한 독립적인 두 건의 감사 결과를 상세하게 서술하고 있다.

연구진은 스마트보안관을 사용하는 청소년과 부모들의 프라이버시와 보안을 위협하는 26건의 취약점을 발견했다. 해당 감사는 2015 시티즌랩 여름연수(CLSI)에 참여했던 연구원들과 보안감사 전문 회사인 Cure53에 의해 수행되었다.

> "전 세계적으로 부모들은 자녀의 SNS와 모바일 기기 사용에 대해 점점 높은 우려를 표시하고 있습니다. 하지만 이번 사례는 선한 의도가 어떻게 매우 잘못된 결과를 초래할 수 있는지 정확하게 보여줍니다. 정부가 권장하는 자녀 관리 S/W는 실제로는 아이들을 보호하는 것이 아니라 더 큰 위험에 노출시키고 있습니다."
> 론 디버트, 토론토 대학교 시티즌랩 소장 및 정치학과 교수

연구진은 '책임있는 공개(responsible disclosure)' 절차에 따라 개발자들에게 취약점을 고지하고, 시의적절하게 문제가 해결되도록 노력했다. 하지만 발표일 현재까지 지적한 문제점들이 보완되었는지는 분명하지 않다.

배경

2015년 4월부터 방송통신위원회(이하 "방통위")가 추진해온, 국내통신사들이 청소년들의 휴대폰에 유해매체물 차단수단을 설치하도록 의무화하는 법령이 시행되었다. 차단수단으로는 여러 종류의 소프트웨어들이 있지만, 그 중에서도 한국무선인터넷산업연합회(MOIBA)가 개발한 스마트보안관이 방통위로부터 홍보 및 예산 상의 지원을 받았다.

스마트보안관은 안드로이드용과 아이폰용이 제공되며 부모가 유해콘텐츠 차단, 앱 관리, 스마트폰 이용시간 관리를 원격으로 할 수 있게 하고 있다.

결과

연구원들은 안드로이드용 스마트보안관의 최신 버전(버전 1.7.5 이하)에서 26건의 보안 취약점들을 발견했다. 보고서는 이러한 취약점들이 스마트보안관 계정 무력화, 데이터 변조, 개인정보 절도 등 사이버공격자에 의해 악용될 수 있다고 설명하고 있다.

프라이버시 및 암호화 문제

연구진이 분석한 버전의 스마트보안관은 이용자 정보를 안전하지 못한 방법으로 저장·전송하고 있었으며, 업계의 암호화 표준을 준수하지 않고 있었다. 이러한 취약성은 공격자가 정보를 모니터링하거나, 정보를 변조하기 위해 서버와 프로그램으로 위장하는 것을 가능하게 한다.

또한 연구진은 지난 5월부터 프라이버시 문제로 스마트보안관의 웹사이트 관리 기능 서비스가 중단되었음에도 불구하고, 스마트보안관이 브라우징 데이터를 MOIBA 서버로 전송하고 있는 것을 발견했다.

인증 문제

연구원들은 계정의 등록과 관리가 적절한 확인절차나 암호 없이도 가능하다는 것을 발견했다. 이 경우 이용자 계정이 도용되거나 탈취

될 수 있다. 공격자는 심지어 스마트보안관이 설치되어 있는 휴대폰의 다른 기능들을 원격으로 조작할 수 있다. 덧붙여 스마트보안관의 자녀폰 관리 기능들은 손쉽게 무력화시키거나 우회할 수 있다.

인프라 문제

연구진은 스마트보안관의 인프라가 적절하게 보호 내지 관리되고 있지 않음을 알아냈다. 보고서에 의하면 서버의 경우 구식 프로그램을 사용하고 있고, 업계 표준의 보안조치 및 암호화가 제대로 구현되지 않고 있었다. 또한 서버는 '무작위 대입 공격(brute force)' 방식의 개인정보 수집 시도나 잘못된 요청을 추적하거나 거부하지 않고 있어 서비스와 이용자들을 심각한 위험에 노출시키고 있다.

> "보안 감사에서 발견된 기술적 문제들은 스마트보안관이 이용자 정보 보호와 프로그램 보안에 있어 가장 일반적인 관행을 준수하는 데 근본적으로 실패했음을 보여주고 있습니다. 이러한 취약점들은 아이들이 보호수단을 회피하거나 악의적인 공격자가 모든 이용자의 기기에 대한 접근에 장애를 일으키고 서비스 운영을 방해하는 것을 매우 쉽게 만들어줍니다. 이러한 실패는 프로그램의 토대부터 아이들의 안전을 고려하지 않았다는 것을 입증할 뿐만 아니라, 더 우려되는 부분은 악용가능성이 수 년간 열려 있었다는 것입니다." – 콜린 앤더슨, 프리랜서 연구원

법적·정책적 함의

> "스마트보안관의 취약점은 이 앱이 한국법 상의 개인정보 보호와 정보 보안 요건을 갖추지 못했다는 사실을 시사하고 있습니다." – 사라 맥큔, 수석법률자문, 시티즌랩

시티즌랩 보고서는 앱의 취약한 설계가 MOIBA의 스마트보안관 약관과 개인정보보호정책에서 주장하는 바와 어긋난다고 지적하고 있다. 또한 연구진에 의하면 스마트보안관의 기능이 2015년 4월 시행 전기통신사업법령의 요구를 초과하여 이용자들의 프라이버시를 침해하고 있다고 한다.

> "정부가 지원하는 이 애플리케이션의 이용자 프라이버시 침해 가능성과 정부의 방침에 의해 널리 사용되고 있다는 사실은 국제인권법상 심각한 우려를 유발합니다." – 사라 맥큔, 수석법률자문, 시티즌랩

불안한 이용자는 어떻게 해야 하는가?

시티즌랩의 이번 보고서 발표는, 현재 및 장래 이용자들과 한국의 규제당국에게 스마트보안관의 보안상 그리고 프라이버시상의 문제에 대해 조언을 하여 사람들이 자신의 정보 보안에 대해 지각있는 선택을 하도록 하기 위함이다.

시티즌랩은 MOIBA에 연락해 연구 결과의 기술적인 세부 사항들을 공유했으며, 이 보고서를 공개하기 전에 문제를 수정할 수 있도록 45일을 기다렸다. 8월 5일 MOIBA의 담당자가 답변을 해왔으며 15건의 취약점을 수정하기 위한 첫 번째 시간표를 제시했다. 8월 6일 MOIBA는 HTTPS를 지원하는 업데이트 버전(v.1.7.6)을 공개했다. 8월 25일 공개된 추가 업데이트(v.1.7.7)에서는 추가적 취약점을 보완했다고 주장했다. 하지만 시티즌랩 연구진에 의하면 2015년 9월 20일 현재까지 취약점들이 전부 보완되었는지 대해 MOIBA가 별도로 확인해준 바는 없다.

연구진은 스마트보안관에 대해 독립적이고 철저한 보안 감사가 이루어지기 전까지는 해당 앱의 추후 사용과 홍보를 중단할 것을 권고한다.

보안성을 염려하는 이용자는 MOIBA에게 직접 연락해 보안 취약점 해결의 진행상황에 대한 구체적인 내용을 문의해보기 바란다(이메일: burdli@moiba.or.kr 홈페이지: https://ss.moiba.or.kr).

최종 보고서 바로 가기

언론사 문의 info@citizenlab.org

Guide on Citing in Media:
Title: Are the Kids Alright? Digital Risks to Minors from South Korea's Smart Sheriff Application
Published By: The Citizen Lab, Munk School of Global Affairs, University of Toronto.
Publication Date: 20 September 2015
Report URL: https://citizenlab.org/2015/09/digital-risks-south-korea-smart-sheriff/

Post a Comment

Your email is *never* shared. Required fields are marked *

Name *

Email *

Website

Comment

Post Comment