여전히 위험에 처해있는 아이들: 시티즌랩의 스마트보안관 보고서 "우리의 아이들은 안전한가"에 대한 업데이트

November 1, 2015

Tagged: Smart Sheriff, South Korea

Categories: Reports and Briefings, Research News

2015년 11월 1일

개요

- 두 번째 스마트보안관 감사에서도 해당 앱의 자녀용과 부모용을 사용하는 이용자들을 심각한 위험에 노출시키는 취약점이 무수히 해결되지 않은 채 남아있음이 확인되었다.
- 스마트보안관을 보급·관리하는 한국무선인터넷산업연합회 MOIBA는 제기된 문제들을 신속히 보완하지 못하였으며 (문제를 인식한지 90일이 넘었음에도 불구하고), 보안 업데이트는 특히 이용자의 보안과 관련된 문제들을 적절하고 효과적으로 해결하지 못했고, MOIBA는 이미 알고 있는 스마트보안관의 위험에 대해 대중에게 투명하게 밝히지 않았다.
- 시티즌랩은 스마트보안관을 지체 없이 오픈마켓에서 내리고, 현재 사용자들은 스마트보안관의 사용을 즉시 중단할 것을 권고한다.

*** 참고**: 2015년 10월 31일 시티즌랩은 MOIBA가 스마트보안관을 구글플레이스토어에서 내린 것을 발견했다. 하지만 스마트보안관 API는 그대로 유지되고 있어서 이용자들을 보안 위험에 노출시킨다. 추가적으로 MOIBA는 구글 플레이 스토어에 스마트보안관을 "사이버안심존"이라는 새로운 이름으로 재출시한 것으로 보인다. 1.7.8 버전에 대한 간단한 검사에서 사이버안심존이 본 보고서에서 다루는 스마트보안관 1.7.7 버전과 외형적인 부분 외에는 기능적으로 동일한 것으로 나타났다. 결론적으로 이 프로그램은 스마트보안관의 모든 보안 문제들을 그대로 가지고 있다.

지난 2015년 9월 20일, 토론토 대학교 뭉크 글로벌상황대학원 산하 시티즌랩 (Munk School of Global Affairs, Citizen Lab)은 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 발표했다. 동 보고서는 한국 정부가 권장하는 유해정보 차단 소프트웨어인 "스마트보안관"의 프라이버시 보호 정도 및 보안성에 대한 독립적인 두 건의 감사 결과를 상세하게 서술하고 있다. 시티즌랩과 독일계 보안감사 전문회사인 Cure 53가 수행한 보안감사에서 스마트보안관을 사용하는 청소년과 부모들의 프라이버시와 보안을 위협하는 26건의 취약점이 발견되었다. 이러한 취약점들은 사이버공격자들이 스마트보안관 계정을 무력화하거나, 데이터를 변조하거나, 전체 이용자 데이터베이스에서 개인정보를 절취하는 데 악용될 수 있다. 또한 스마트보안관과 관련된 법적, 정책적 문제점들도 지적되었다. 보고서에는 상세한 기술적[pdf] 및 법적·정책적[pdf] 부록이 첨부되어 있다. 2015년 8월에 수행된 Cure53의 첫 번째 감사 결과는 여기 [pdf]에서 확인할 수 있다.

보고서를 작성하는 동안, 시티즌랩은 '책임있는 공개(responsible disclosure)' 절차에 따라 스마트보안관을 개발한 MOIBA에게 관련 내용을 고지했다. 당시 시티즌랩은 MOIBA에게 서비스를 중단하거나, 어플리케이션의 문제점을 수정하는데 필요한 기간을 제시해달라고 요청했다. MOIBA은 어플리케이션을 중단시키는 대신 9월말까지 모든 문제점을 수정하겠다고 답변했다. 또한 MOIBA는 보안감사에서 발견된 문제점들을 인정했으며, 보고서의 어떠한 내용에 대해서도 이의를 제기하지 않았다. 시티즌랩과 MOIBA는 취약점들에 대해 수차례 연락을 주고받았고, MOIBA가 취약점을 보완하기 위해 필요한 합리적인 기간에 대해 논의했다. 그 과정에서 MOIBA는 자신들이 어플리케이션의 원개발자가 아니며, 스마트보안관의 모든 개발사항에 대해서는 외부 개발자에 의존하고 있어 시티즌랩의 우려를 해결할만한 자체 개발능력이 없다고 밝혔다.

이후 시티즌랩은 여러 번 연락을 시도했으나 MOIBA로부터 답이 오지 않아 9월 20일 보고서를 발표하게 되었다. 보고서에서 시티즌랩은 "MOIBA가 취약점을 어떻게 보완했는지에 대해 충분히 알려주지 않았다"는 점을 지적했고, "스마트보안관에 대해 독립적이고 철저한 보안 감사가 이루어지기 전까지는 해당 앱의 추후 사용과 홍보를 자제"할 것을 촉구했다. MOIBA는 시티즌랩 보고서 발표에 대한 언론보도에서 "즉시 조치를 취했다"고 주장하여, 스마트보안관의 취약점들이 제대로 수정된 것과 같은 인상을 주었다.

후속 감사

2015년 10월 초 Cure 53는 스마트보안관에 대해 2차 감사를 수행했다. 2차 감사는 구글 플레이에서 다운로드한 1.7.7 버전을 대상으로 했다. 2차 감사로부터 스마트보안관 앱에 심각한 문제점들이 아직 남아있음을 시사하고 MOIBA가 취약점을 보완하려고 충분한 노

력을 기울였는지에 대해 의문을 갖게 하는 매우 우려스러운 결과가 나왔다.

스마트보안관이 여전히 가지고 있는 일반적인 위험은 아래와 같다:

- 공격자가 청소년의 휴대폰 번호를 알고 있다면 청소년의 생년월일, 청소년의 휴대폰에 설치된 모든 앱의 목록, 그리고 모든 차단 규칙을 취득할 수 있다.
- 공격자는 여전히 청소년의 휴대폰의 차단 규칙이나 설정을 마음대로 변경할 수 있기 때문에 청소년이 휴대폰을 사용하지 못하도록 잠글 수 있다.
- 공격자는 여전히 스마트보안관 부모용의 비밀번호와 청소년의 계정과 연계된 부모의 휴대폰 번호를 찾아낼 수 있다.
- 스마트보안관의 신 버전들은 모든 API 요청데이터에 대한 암호화를 구현했으나, 이 암호화는 고정된 대칭키를 사용하고 있다. 공격자는 소스코드를 디컴파일해서 해당 키를 찾아 암호화를 무력화시킬 수 있다.
- 스마트보안관의 신 버전들은 MOIBA서버와 통신시 HTTPS를 사용하지만, 여전히 인증서의 유효성을 검증하지 않고 있다. 이미 반복적으로 MOIBA에게 제기한 문제이다. 이 문제는 최초 보고서에서도 설명한 바와 같이 스마트보안관이 여전히 “중간자 (MITM)” 공격에 취약하다는 것을 의미한다.

매우 중요하다고 판단된 문제들의 현재 상태

문제 번호	문제 요약	현재 상태	여전히 공격이 가능한지 여부
1.1	앱과 MOIBA 서버 간의 전송보안 부재	HTTPS 추가됐으나 인증서 검증을 하지 않아 보완이 소용 없음	예
1.2	안전하지 않은 웹뷰로 중간자 공격 가능	문제 1.1이 해결되지 않아 중간자 공격 여전히 가능	예
1.3	이용자 트래픽이 암호화되지 않은 채 노출됨	고정된 AES 키 사용은 이용자트래픽이 일반 관찰자에게는 쉽게 읽히지 않겠지만, 작심한 공격자에게는 정보가 노출된다는 의미임	예
2.2	부모 비밀번호 노출	비밀번호를 은폐하기 위한 보안이 이루어졌지만 쉽게 우회될 수 있음	예
3.1	예측가능한 식별자에 의한 API 식별	식별자 여전히 존재, API 요청은 암호화되었지만 문제 1.3이 계속 존재함에 따라 작심한 공격자는 이 식별자들을 찾아낼 수 있음	예
3.2	API 쿼리가 인증을 거치지 않음	원 보고서 이후 변화 없음	예
3.3	불특정이용자가 보호설정을 변경할 수 있음	원 보고서 이후 변화 없음	예
3.5	불특정이용자가 불특정 번호를 등록하여 이용할 수 있음	시험하지 않았음	판단 불가
3.9	부모용 관리 웹UI를 통해 공격자가 기기설정을 변경하거나 개인정보를 취득할 수 있었음	이전에는 개인식별정보를 노출시켰던 페이지가 404로 답함	아니요
3.10	부모용 관리 웹UI를 통해 공격자가 계정설정을 변경할 수 있었음	이전에는 개인식별정보를 노출시켰던 페이지가 404로 답함	아니요

종합적으로, 시티즌랩과 MOIBA 간의 최초 공개에 대한 대처로 몇 가지 수정 및 보완이 이루어졌지만, 구 버전들과 마찬가지로 신 버전에서도 공격자들이 취약점을 악용할 수 있는 가능성은 거의 동일하다. 또한 민감한 개인정보 및 전송 보안의 보호 결여를 포함하여, 1차 보고서에서 중요하다고 강조된 많은 문제들이 제대로 해결되지 않은 채 남아 있었다. 단 한 가지 성공적으로 수정된 사항이라면 청소년들이 필터링을 우회하는 방법과 관련된 것이다(예컨대 기술적 부록에서 언급한 문제 2.1 등). API 요청 인증 결여와 같은 시스템적 문제들도 여전하다. 전송 보안과 같은 다른 문제들은 매우 불완전하게 수정되어 보안 혜택을 무력화한다.

요약하면, MOIBA는 네트워크에 영향을 미칠 수 있는 서버 문제나 백엔드 취약점 몇 가지를 수정하려 했을 뿐, 어플리케이션을 사용하는 이용자들의 프라이버시나 보안에 직접 영향을 미치는 취약점들은 제대로 수정하지 못했다.

향후 계획

2015년 10월 31일에 공개된 Cure53의 후속 감사는 여기에서 확인할 수 있다. 시티즌랩은 보고서 공개에 따른 MOIBA의 대응과 스마트보안관 1.7.7 버전의 보안 문제가 업데이트를 통해 수정되는지 여부를 지켜볼 것이다.

시티즌랩과 Cure 53는 그 동안 스마트보안관을 지체 없이 오픈마켓에서 내리고, 현재 사용자들은 스마트보안관의 사용을 즉시 중단할 것을 권고한다.

맺음말

스마트보안관 사례는 모든 어플리케이션, 그 중에서도 특히 취약한 어린 청소년들과 다른 이용자들이 사용하는 어플리케이션의 프라이버시 보호 정도와 보안성 검사의 중요성을 잘 보여준다.

또한 보다 광범위한 공공정책의 문제도 드러낸다. 정부가 사용을 강제하는 어플리케이션들은 많은 이용자를 모으게 되고, 많은 이용자들은 많은 잠재적 공격자들을 유인한다는 것이다. 정부가 국민들에게 특정 어플리케이션의 사용을 강제하는 경우에는 반드시 투명하고 책임있는 절차에 의한 보안성과 프라이버시 보호에 대한 특별히 엄격한 실사가 이루어져야 한다.

모든 면에서 스마트보안관은 실패작이다. 스마트보안관을 보급·관리하는 한국무선인터넷산업연합회 MOIBA는 제기된 문제들을 신속히 보완하지 못하였으며 (문제를 인식한지 90일이 넘었음에도 불구하고), 보안 업데이트는 특히 이용자의 보안과 관련된 문제들을 적절하고 효과적으로 해결하지 못했고, MOIBA는 이미 알고 있는 스마트보안관의 위험에 대해 대중에게 투명하게 밝히지 않았다.

스마트보안관은 취약한 집단을 보호하기 위한 시도로써 특정 어플리케이션을 강제해 오히려 그 집단을 위험에 노출시킨 사안으로 교훈적인 연구 사례가 될 것이다. 3개월간의 연구와 후속 조사의 결과, 정책의 초기 의도가 무엇이었든지 간에 이용자의 보안과 프라이버시 보호를 위해서는 스마트보안관을 사용하는 것 보다 당장 삭제하는 것이 바람직하다.

Post a Comment

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

Name *

Email *

Website

Comment

Post Comment