공유기 제품 생산 시 적용할 보안 가이드

2015. 6

KISA
한국인터넷진흥원

목 차

제1장
개요

제1장 개요

1. 배경

인터넷 공유기[1] 사용이 급증함에 따라 보안설정이 미흡한 공유기를 통한 금융정보 유출, DDoS 등의 다양한 공격이 발생하고 있다. 최근 커피숍 등 공공영역에서 공유기 DNS 변조를 통하여 사용자를 파밍 사이트로 유도하는 등 사용자 개인정보 유출에 대한 이슈가 발생하였으며, 사설 공유기를 통한 통신사 DNS DDoS 공격이 발견되는 등 대규모 DDoS 공격을 위한 새로운 위협으로 부상되고 있다.

공유기는 통신사가 제공하는 '관리형 공유기'와 이용자가 직접 구매·설치하는 '사설 공유기'로 구분되어 인터넷망에서 사용되고 있다. 관리형 공유기는 통신사가 자체 보안 규격에 따라 인증시험을 거쳐 보급되고 있으며, 보안취약점이 발생할 경우 원격으로 보안 업데이트가 가능하다. 허나 사설 공유기의 경우 별도의 인증 없이 제작·유통되고 있으며, 접속 인증 시 취약한 ID/PW가 초기 상태로 설정되어 있어 보안에 취약한 상태로 노출되어 있다.

이러한 이슈는 제조사에서 제품 설계 시 보안을 고려하지 않은 것이 가장 큰 원인이나, 공유기를 사용함에 있어 보안 설정을 하지 않는 사용자도 원인으로 볼 수 있다. 2013년 실시한 '무선랜 보안인식 조사결과'에 의하면, 공유기 사용자의 경우 최초 설치 이후 보안설정을 하지 않는 등 보안 설정 인식에 비해 보안 실천이 부족한 실정이다.

이에 본 가이드에서는 공유기를 통해 발생 가능한 보안 위협을 다루어 그 위험성을 인지하도록 하며, 제조사에서 제품 설계·개발 시 반영하여야 할 사항을 제공함으로써 사고를 예방하고 발생할 수 있는 피해를 최소화하고자 한다.

---

1) 공유기 : 컴퓨터, TV, 전화 등의 다양한 기기를 인터넷선과 연결해주는 중간매개체로 각 기기들이 인터넷을 접속할 수 있도록 해주는 기기

2. 가이드 목적 및 구성

목적	- 공유기 관련 위협 심각성 인지를 통한 보안 인식 제고 - 안전한 공유기 설계·개발을 통한 침해사고 예방 및 피해 최소화
대상	- 공유기 제조사 개발자
범위	- 공유기 설계, 제작, 관리 시 지켜야 할 사항
구성	- [1장] 개요 1.1 배경 1.2 가이드 목적 및 구성 - [2장] 보안 위협 2.1 통신 내용 유출 2.2 DDoS 공격 악용 2.3 DNS 변조 - [3장] 공유기 제품 생산 시 적용할 보안가이드 - [4장] 공유기 보안가이드 해설

제2장
보안 위협

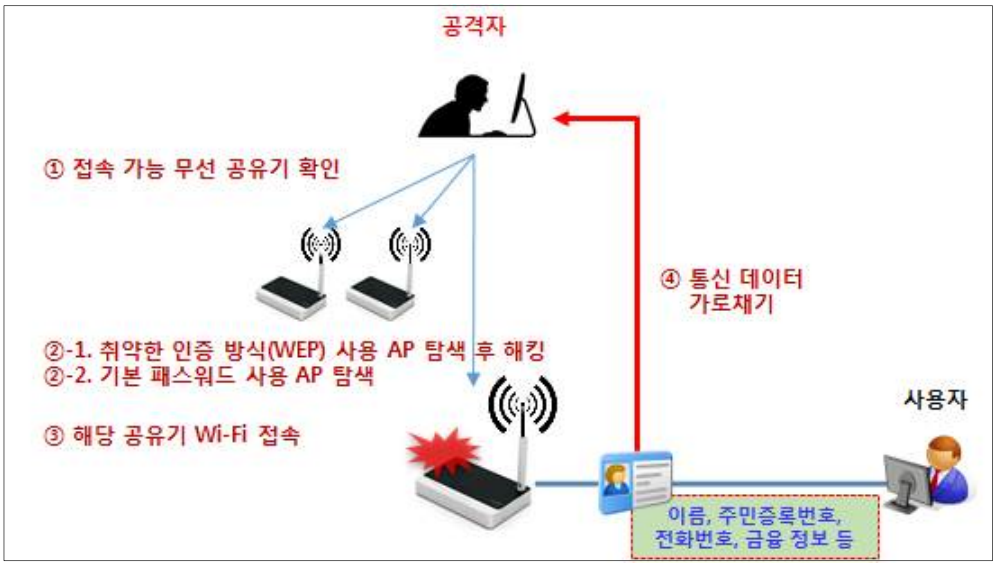
제2장 보안 위협

2.1 통신 내용 유출

상당수의 공유기 사용자의 경우 무선 인증 패스워드를 기본으로 설정하거나 취약한 인증방식(WEP[2])을 사용하고 있어, 공격자는 해당 공유기를 통해 제공되는 무선 네트워크에 접속할 수 있다. 이후 ARP 스푸핑(ARP Spoofing)[3] 등의 공격 기법을 통해 평문으로 전송되는 사용자의 계정, 금융 정보 등 개인정보를 탈취할 수 있다.

실제 의료기관의 무선 인터넷에 접속하여 환자의 진료기록 등 개인정보를 유출하거나 기업 네트워크를 해킹하여 고객의 신용카드 리스트 등 정보를 획득하려다 적발되는 등 Wifi를 악용한 다수의 사례가 존재한다.

<그림 2-1> 취약 공유기 통한 통신 내용 유출



2) WEP(Wired Equivalent Privacy) : 초기 무선랜 보안설정 방법으로 유선랜과 동등한 수준의 보안성 제공의 목적으로 만들어진 보안기술이다. 대칭키 기반 암호화 기법으로 현재는 암호 알고리즘 자체의 취약성이 많이 알려져 있어 사용이 권고되지 않는다.
3) ARP 스푸핑(ARP Spoofing) : 주소 결정 프로토콜(ARP, Address Resolution Protocol) 메시지를 이용하여 상대방의 데이터 패킷을 중간에 가로채는 중간자 공격 기법을 말한다.

2.2 DDoS 공격 악용

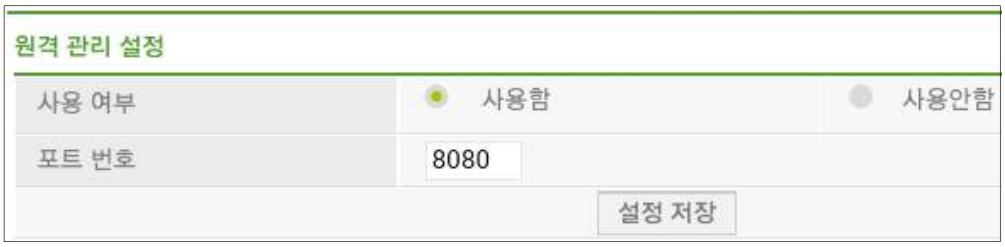
일부 공유기의 경우 유지보수를 위해 텔넷(Telnet) 포트를 사용하고 있는데, 관리 편의성을 위하여 계정 및 패스워드를 기본 혹은 추측하기 쉬운 패스워드로 사용하는 경우가 많다. 이런 경우 공격자는 취약한 계정 및 패스워드 정보를 이용하여 공유기 텔넷 서비스에 접속, 악성코드를 다운로드하여 감염시킬 수 있다. 이후 공격자는 다양한 공격을 수행할 수 있는데, 대표적인 사례로 최근 발생하였던 감염된 다수의 공유기를 통한 통신사 DDoS 공격이 있다.

<그림 2-2> 텔넷 접속 통한 DDoS 공격용 악성코드 설치

2.3 DNS 변조

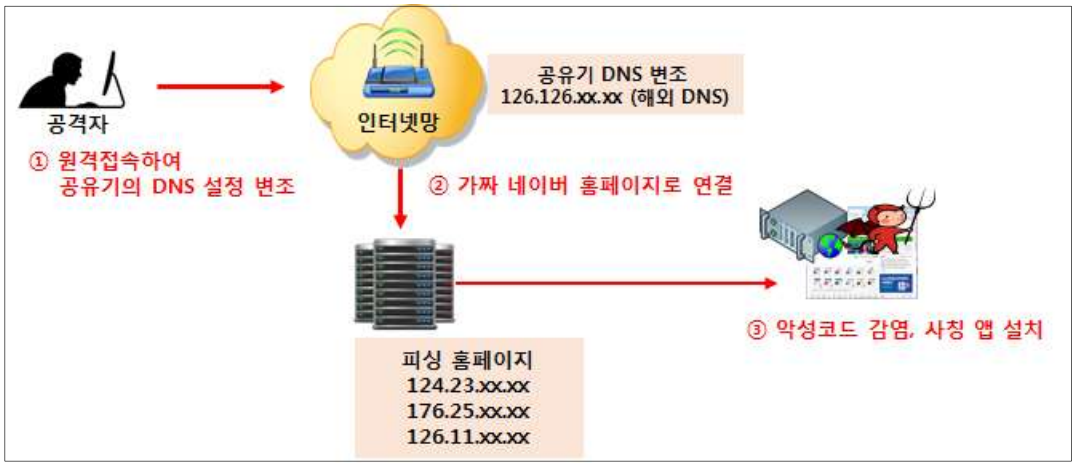
공유기 설정에서 원격 접속이 허용되어 있을 경우 공격자는 원격에서 공유기 관리자 페이지에 대한 접근이 가능하다. 상당수의 사용자가 이 관리자 페이지에 대해 별도로 패스워드를 설정하지 않거나 혹은 기본 패스워드를 사용하고 있어 공격자는 손쉽게 해당 페이지에 접속하여 설정 변경을 통한 공격을 수행할 수 있게 된다.

<그림 2-3> 공유기 관리페이지 - 원격 관리 설정



가장 흔히 발견되는 사례의 경우 인터넷에서 접속 가능한 공유기의 DNS 주소를 변조하는 방법으로 이로 통해 해당 공유기 사용자는 사칭앱 유포, 금융정보 유출등의 피해를 입을 수 있다.

<그림 2-4> 공유기 DNS 설정 변조를 통한 피싱



이외에도 최근 공유기 취약점을 이용한 CSRF[4] 스크립트가 공개되어 이슈가 되고 있다. 공격자에 의해 해당 스크립트가 삽입된 웹페이지를 공유기 사용자가 방문할 경우 원격 접속이 허용되지 않은 공유기라도 CSRF 스크립트에 의해 DNS 주소가 변조되게 된다.

<그림 2-5> CSRF 스크립트를 통한 공유기 DNS 변조

4) CSRF(Cross-Site Request Forgery) : 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 수행하도록 하는 공격

제3장
공유기 제품 생산 시 적용할 보안가이드

제3장 공유기 제품 생산 시 적용할 보안가이드

구분	구현항목
접근성	① 고객이 공유기 보안설정을 쉽게 할 수 있도록 직관적인 사용자 인터페이스와 매뉴얼을 제공하여야 한다.
접근통제	② 공유기 관리자 페이지에 대한 원격 접속을 기본으로 허용하지 않아야 한다.
	③ 공유기의 관리자 페이지 접속 시에는 ID와 비밀번호(PW) 없이 접속할 수 없도록 하여야 한다.
	④ 무선(Wi-Fi) 인증시에도 비밀번호 없이 접속할 수 없도록 비밀번호 사용을 기본 설정하여야 한다.
	⑤ 공유기의 관리자 페이지 및 무선 인증 시 최초 ID와 PW의 경우 제품마다 다르게 하거나 비밀번호를 설정하여야 공유기를 사용가능하도록 하여야 한다.
서비스 보안관리	⑥ 모든 비밀번호(최초, 변경 모두 해당)는 영문, 숫자, 특수문자를 포함하여 8자 이상으로 하여야 하며, 비밀번호 설정 창에도 복잡도가 높은 문구로 설정하도록 사용자에게 안내하여야 한다.
	⑦ 불필요한 외부 접속 포트나 Telnet, FTP, 등의 서비스는 비활성화 한다. 반드시 필요할 경우에는 비밀번호를 설정하여야 사용 가능하도록 한다.
	⑧ 고객 지원 목적의 접속 포트를 제거하고 필요하다면 접근 IP 제한 등 추가적인 보안 조치 방안을 마련한다. 유지 보수 등을 위해 공유기에 백도어 기능을 포함하지 않도록 한다.
	⑨ 모든 관리자 페이지는 인증 후에 접근할 수 있도록 세션 인증 등을 구현한다. 세션 인증 구현 시 예측 가능한 세션 ID 값을 사용하지 않도록 한다.
	⑩ 관리자 페이지에서 시스템 명령어 실행 기능을 제공하지 않도록 한다. 다만, 반드시 필요할 경우 지정한 특정 명령어만 실행하도록 제한한다.
암호화	⑪ 무선 암호화 방식은 보안강도가 높은 WPA2가 기본 설정되도록 하여야 한다.
펌웨어 보안	⑫ 공유기 펌웨어 업데이트가 발생하는 경우 사용자가 인지할 수 있는 방안을 강구하여야 한다.
	⑬ 공유기 펌웨어 업데이트 시 파일 고유 해시값을 비교하여 변조 여부에 대한 무결성 검증을 실시할 수 있도록 한다. 무결성 인증 시 SHA-256 이상의 암호화 알고리즘을 사용하도록 한다.

제4장
공유기 보안가이드 항목 해설서

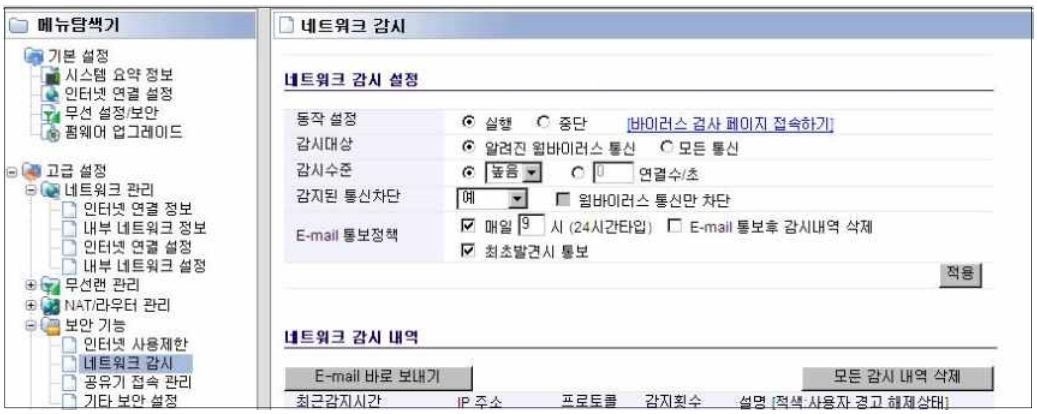
제4장 공유기 보안가이드 항목 해설서

■ 접근성

① 고객이 공유기 보안설정을 쉽게 할 수 있도록 직관적인 사용자 인터페이스와 매뉴얼을 제공하여야 한다.

공유기의 경우 각종 설정을 위한 관리자 페이지가 제공되며, 해당 페이지를 통해 IP에서부터 보안 항목 등 다양한 부문에 대해 설정이 가능하다. 허나 현재 시중에 유통되고 있는 공유기 내 관리자 페이지는 일반 고객들이 보안 설정을 하기에 많은 어려움이 존재한다. 설정과 관련된 용어도 생소할뿐더러 해당 내용에 대해 별도로 설명이 명시되어 있지 않은 경우가 있어 고객으로 하여금 보안 설정의 불편함을 가중시키고 있다.

<그림 4-1> 공유기 관리자 화면



이에 제조사는 고객들이 보안설정을 쉽게 할 수 있도록 직관적인 사용자 인터페이스를 제공하여야 한다. 또한 각 설정 항목별로 설명 내용을 해당 페이지에 명시하거나 별도 매뉴얼로 제공하여 고객들이 손쉽게 보안설정을 할 수 있도록 한다.

■ 접근통제

② 공유기 관리자 페이지에 대한 원격 접속을 기본으로 허용하지 않아야 한다.

공유기 관리자 페이지에 대한 외부 원격 접속 기능을 기본 설정으로 허용하지 않는다. 외부 원격 접속 기능이 활성화 되어 있을 경우 공격자는 원격에서 이를 통해 관리자 페이지에 접속하여 공격에 필요한 기능을 설정할 수 있으므로, 로컬 네트워크에서만 접속이 가능하도록 하며, 고객이 필요로 할 시 설정을 통해 활성화 후 사용할 수 있도록 한다.

③ 공유기의 관리자 페이지 접속 시에는 ID와 비밀번호(PW) 없이 접속할 수 없도록 하여야 한다.
④ 무선(Wi-Fi) 인증시에도 비밀번호 없이 접속할 수 없도록 비밀번호 사용을 기본 설정하여야 한다.
⑤ 공유기의 관리자 페이지 및 무선 인증 시 최초 ID와 PW의 경우 제품마다 다르게 하거나 비밀번호를 설정하여야 공유기를 사용가능하도록 하여야 한다.

장비의 출고 시 초기 관리자의 ID/패스워드 및 무선인증 패스워드가 설정되어 있지 않거나 관리자 ID/패스워드를 admin/admin과 같이 설정되어 있는 상태, 무선인증 패스워드가 12345678 등과 같이 유추하기 쉽게 설정되어 있는 상태는 암호화 설정을 하지 않은 보안수준에 해당한다. 이에 관리자 ID/패스워드 및 무선인증 패스워드의 경우 설정 없이 접속할 수 없도록 기본 설정으로 하여야 하며, 최초 설정의 경우도 제품마다 다르게 하거나 혹은 패스워드를 설정하여야 공유기를 사용가능하도록 하여야 한다.

<그림 4-2> 취약한 패스워드 사용 예

⑥ 모든 비밀번호(최초, 변경 모두 해당)는 영문, 숫자, 특수문자를 포함하여 8자 이상으로 하여야 하며, 비밀번호 설정 창에도 복잡도가 높은 문구로 설정하도록 사용자에게 안내하여야 한다.

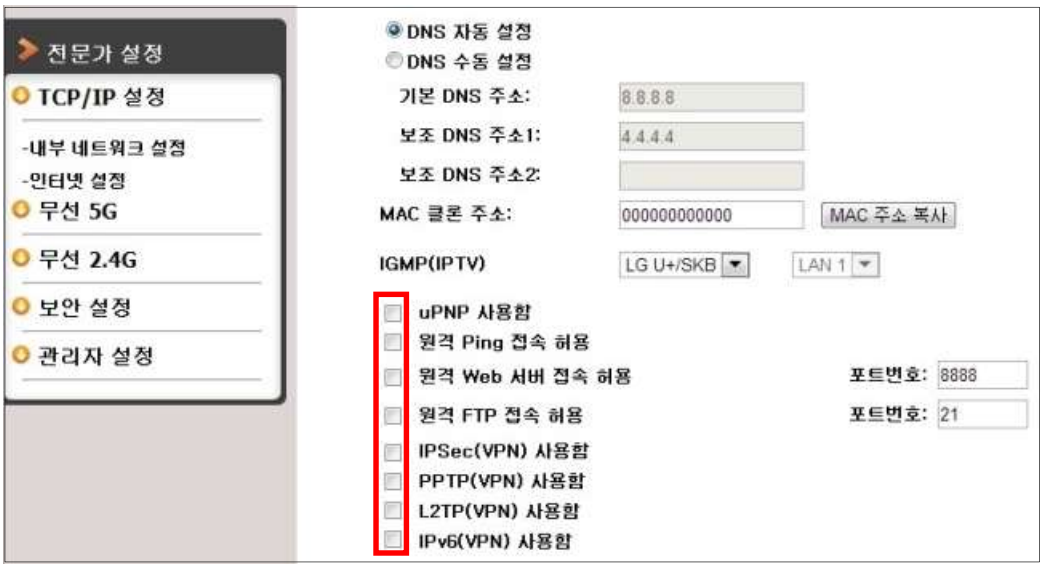
비밀번호 설정의 경우 다음과 같이 사용자에게 안내하도록 한다.

<그림 4-3> 패스워드 설정방법 안내 예

■ 서비스 보안관리

⑦ 불필요한 외부 접속 포트나 Telnet, FTP 등의 서비스는 비활성화 한다.
반드시 필요할 경우에는 비밀번호를 설정하여야 사용 가능하도록 한다.

<그림 4-4> 불필요 서비스 비활성화

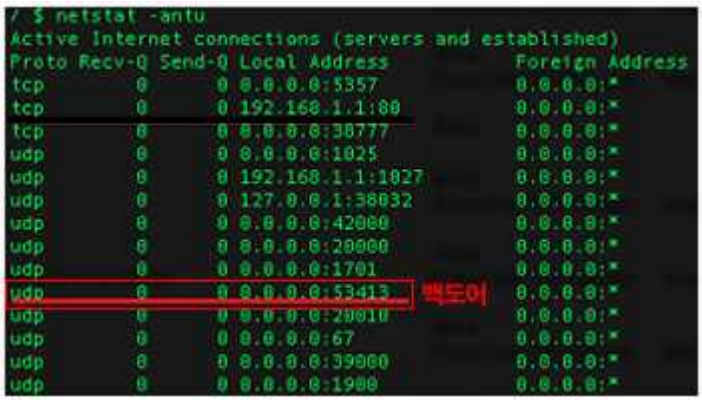


불필요한 외부 접속 포트나 텔넷, FTP 등의 서비스의 경우 기본으로 활성화 되지 않도록 한다. 불필요하게 여러 포트가 열려있거나 서비스가 실행 될 시 공격자에게 공유기에 접속하거나 공격을 할 수 있게 만드는 수단이 될 수 있다. 반드시 필요로 할 경우에는 비밀번호 설정 등 접근통제를 하여야 사용 가능하도록 제한하여야 한다.

⑧ 고객 지원 목적의 접속 포트를 제거하고 필요하다면 접근 IP 제한 등 추가적인 보안 조치 방안을 마련한다. 유지 보수 등을 위해 공유기에 백도어 기능을 포함하지 않도록 한다.

일부 공유기의 경우 고객 지원 목적으로 접속 포트를 열어놓는 경우가 있는데, 이 역시 공격에 악용될 소지가 있으므로 해당 포트를 제거하도록 하며 필요 시 접근 IP제한 등 추가적인 보안 조치 방안을 마련하도록 한다. 또한 일반 관리자 계정이 아닌 유지 보수 목적의 임의 계정과 백도어 기능을 공유기에 포함하지 않도록 한다.

<그림 4-5> 특정 공유기 내 백도어 설치 사례



⑨ 모든 관리자 페이지는 인증 후에 접근할 수 있도록 세션 인증 등을 구현한다. 세션 인증 구현 시 예측 가능한 세션 ID 값을 사용하지 않도록 한다.

관리자 페이지는 인증 후에 접근할 수 있도록 이에 필요한 세션 인증 등을 구현한다. 세션 ID에 일정한 공식 값을 사용하거나, 한번 사용했던 값이 재사용되는 등 예측 가능한 세션 ID값을 사용할 경우 무차별 대입 공격(Brute Force)에 취약할 수 있으므로, 랜덤한 값을 할당하여 추측을 어렵게 하여야 한다.

⑩ 관리자 페이지에서 시스템 명령어 실행 기능을 제공하지 않도록 한다.
다만, 반드시 필요할 경우 지정한 특정 명령어만 실행하도록 제한한다.

관리자 페이지에서 시스템 명령어 실행 기능을 제공하지 않도록 한다. 시스템 명령어 실행 기능이 활성화되어 있을 시 공격자는 이를 이용하여 공유기를 대상으로 공격 명령을 수행할 수 있다. 단 반드시 필요할 경우 지정한 특정 명령어만 실행하도록 제한한다.

<그림 4-6> 특정 공유기 내 명령어 실행 화면

■ 암호화

⑪ 무선 암호화 방식은 보안강도가 높은 WPA2가 기본 설정되도록 하여야 한다.

전송데이터 보안은 일반적으로 무선 클라이언트와 무선 AP와의 구간에서의 보안성 유지를 위해 전송 데이터 암호화를 사용해야 한다. 암호화는 보안 강도에 따라 WEP, WPA, WPA2 등으로 분류되며, 보안강도가 낮을수록 보안상 문제가 발생할 소지가 높다. 이에 제조사는 제품 설계 시 보안강도가 높은 WPA2를 기본으로 설정되도록 하여야 한다.

<그림 4-7> 무선 인증/암호화 기술별 특징

구분	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access2)
인증	• 사전 공유된 비밀키 사용 (64비트, 128비트)	• 사전에 공유된 비밀키를 사용하거나 별도의 인증서버를 이용	• 사전에 공유된 비밀키를 사용하거나 별도의 인증서버를 이용
암호화	• 고정 암호키 사용 (인증키와 동일) • RC4 알고리즘 사용	• 암호키 동적 변경(TKIP) • RC4 알고리즘 사용	• 암호키 동적 변경 • AES 등 강력한 블록 암호 알고리즘 사용
보안성	• 64비트 WEP 키는 수분내 노출 • 취약하여 널리 쓰이지 않음	• WEP 방식보다 안전하나 불완전한 RC4 알고리즘 사용	• 가장 강력한 보안기능 제공

■ 펌웨어 보안

⑫ 공유기 펌웨어 업데이트가 발생하는 경우 사용자가 인지할 수 있는 방안을 강구하여야 한다.

공유기 펌웨어 업데이트가 발생하는 경우 사용자가 인지할 수 있는 방안을 강구하여야 한다. 현재 시중에 유통되고 있는 공유기의 경우 새로운 버전의 펌웨어가 출시되더라도 고객은 공유기 관리페이지에서 업데이트 확인을 하거나 제조사 홈페이지를 통해 알리고 있다.

이로 인해 사용자는 현재 자신이 소유하고 있는 공유기가 최신 버전인지에 대한 확인이 어려운 문제가 발생하므로 제조사는 업데이트가 발생하는 즉시 일정기간 홈페이지 팝업 안내 및 이메일 알림 등을 통해 사용자에게 이를 알려야 한다.

⑬ 공유기 펌웨어 업데이트 시 파일 고유 해시값을 비교하여 변조 여부에 대한 무결성 검증을 실시할 수 있도록 한다. 무결성 인증 시 SHA-256 이상의 암호화 알고리즘을 사용하도록 한다.

공유기 펌웨어가 공격자의 의해 변조될 경우 이를 통해 수많은 공유기가 추가적으로 공격에 악용되어 사회적으로 큰 보안 위협을 야기할 수 있다. 이에 제조사는 펌웨어 무결성 검증 등을 통해 사용자가 안전하게 업데이트 할 수 있도록 서비스를 제공하여야 하며, 무결성 인증 시 SHA-256 이상의 암호화 알고리즘을 사용하여 보안성을 강화하도록 한다.