LACNOG- M³AAWG 공동 작성

CPE(가입자 댁내장치) 최소 보안 요구사항에 대한

Best Current Operational Practices

LAC-BCOP-1

2019 년 5 월

이 문서는 LACNOG 웹사이트에서 다운로드 가능합니다. www.lacnog.net/docs/lac-bcop-1

이 문서는 M³AAWG 웹사이트에서 다운로드 가능합니다. www.m3aawg.org/CPESecurityBP

이 문서는 M³AAWG 웹사이트에서 다운로드 가능합니다. www.m3aawg.org/CPESecurityBP-Korean

이 문서는 LACNOG[1] (Latin American and Caribbean Network Operators Group) 와 M³AAWG[2] (Messaging, Malware and Mobile Anti-Abuse Working Group).가 공동으로 작성한 Best Current Operational Practices (BCOP)이다. 이는 LACNOG 워킹그룹 LAC-AAWG[3] (Latin American and Caribbean Anti-Abuse Working Group) 와 BCOP Working Group[4]의 원본을 토대로 M³AAWG 회원들과 Senior Technical Advisors, M³AAWG Technical Committee 의 협력에 의해 작성되었다.

차례

[1] The Latin American and Caribbean Network Operators Group (LACNOG), https://www.lacnog.net/
[2] Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG), https://www.m3aawg.org/
[3] Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG), https://www.lacnog.net/lac-aawg/
[4] LACNOG BCOP Working Group, https://www.lacnog.net/wg-bcops/

요약

CPE(Customer Premise Equipment : 가입자 댁내장치) 란 사용자가 계약한 인터넷 서비스 제공자(ISP)의 네트워크에 접속하기 위해 이용하는 통신기기를 뜻한다. CPE 의 예를 들면 모뎀(케이블, xDSL, 광케이블) 및 무선 공유기 등이 있다.

내장 소프트웨어와 초기설정의 보안상 취약성으로 인해 CPE 는 부적절하게 설정된 서비스와 기본 설정된 인증정보의 악용으로부터 멀웨어에 의한 완벽한 통제에 이르기까지 다양한 공격의 대상이 되어 왔다. 이들 공격의 주요 목적은 DoS 공격의 제어, 무허가 암호통화의 채굴, 멀웨어의 배포, 스팸, 피싱, 인증정보의 탈취 등이다.

일반적으로 보안상 취약성에는 다음과 같은 것들이 포함된다.

- 수많은 디바이스에서 공통으로 사용되는 인증정보
- 변경 불가능한 인증정보(하드코딩)
- 쓸모없거나 안전하지 않은 프로토콜과 알고리듬의 사용
- 명시되지 않은 액세스(백도어)
- 보안상의 문제점을 해결하기 위한 자동화되었고 보안적으로 안전한 업데이트의 결여
- 디폴트 설정에서 유효화된 불필요 및 보안상 안전하지 않은 서비스
- 무효화할 수 없는 서비스
- 보안상 안전하지 않은 원격 제어

이 문서는 ISP 가 CPE 를 구입할 때 그것이 보안상 안전한 초기설정 및 원격 관리수법과 업데이트 기능을 보유하고 있음을 확인하기 위한 보안 요구사항의 최소 사항을 명시하는 것을 목적으로 한다. 이 문서의 목표는 공급자의 네트워크와 인터넷 전체의 침해 리스트를 절감해 서비스의 품질저하 및 사용 불능, 기술 지원 및 복구작업과 같이 기기 악용으로 발생하는 공급자의 금전적 부담과 영향을 최소한으로 억제하기 위함이다.

CPE 가 지원해야 하는 완벽한 기능 목록 또는 하드웨어 및 소프트웨어의 명세를 제공하는 것은 이 문서의 목적이 아니다. 또한 이 문서는 편의상 Ipv6 프로토콜과 Ipv4 프로토콜이 지원되어 기능이 구현되어 있을 경우 유효화된 상태일 것을 가정하여 작성되었다.[5].

1. 용어 설명

이 문서에서 사용되는 용어와 그 내용은 다음과 같다.

1. CPE(Customer Premise Equipment : 가입자 댁내장치): 이 장치는 고객이 인터넷서비스 제공자(ISP)의 네트워크에 접속하기 위해 사용하는 통신기기를 뜻한다. 이러한 종류의 기기는 커스터머 에지(CE) 라우터, 주택용 게이트웨어(RG) 등으로 표기되는 일도 있다.

[5] CPE 의 구매 요구사항에 IPv6 에 대한 기술지원과 구현에 관한 요구를 포함하지 않을 경우 ISP 가 고객에게 IPv6 접속을 제공하지 않을 수 있다. 이는 ISP 에게 있어 IPv4 주소 고갈로 인한 비지니스 리스크로 번질 위험이 있다.

2. 펌웨어(Firmware): CPE 에서 동작하는 소프트웨어로 OS,네트워크 인터페이스 소프트웨어 및 소프트웨어 패키지와 서비스, 그리고 그에 대한 설정을 포함한다.

3. 백도어(Backdoor):시스템 또는 그 데이터에 대해, 명세서에 기대되지 않은 방법으로 액세스 가능하게 하는 모든 메카니즘을 말한다. 백도어의 예를 들면, 비밀번호 없이 하드코딩된 사용자명, 고정된 비밀번호 또는 예상 가능한 해당 날짜의 비밀번호(password-of-the-day), 인증없이 관리기능을 실행하도록 만드는 명시하지 않은 서비스 등이 있다. 백도어는 고의적으로(나중에 액세스 가능하도록 설계된) 또는 고의적이지 않은(개발목적으로 사용된 후 우연히 펌웨어의 일반기능으로 들어가게 된) 경우가 있다. 백도어는 또한 좋지 않은 프로그래밍 습관으로 인해 발생하는 경우가 있다.

4. 적절한 암호화/암호수법: Internet Engineering Task Force (IETF) 또는 다른 표준화 단체에 의해 공개된 최신 버전의 오픈 스탠더드 암호화 알고리듬/프로토콜. 이를 구현하기 위해서는 최신 암호기술과 키 사이즈를 선택할 수 있게 해야 한다.

5. 하드코딩된 인증정보: 소스코드에 패치를 적용(그 결과 새로운 바이너리/펌웨어를 릴리스하는)하지 않으면 변경 불가능하거나 무효화할 수 없는 제품 소스코드의 공통 인증정보(해당 제품의 모든 기능 구현에서 공통).

6. 서비스(서버타입 프로세스 또는 데몬): 필요할 때에만 서비스에 쿼리를 실행하는 클라이언트 소프트웨어가 아닌 특정 포트에 대하여 액티브한 상태로 접속을 대기하는 서버 프로세스.

7. 디폴트(DEFAULT): 판매자에 의한 기본 설정.

8. 이 문서에서 사용되는 키워드 "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", "OPTIONAL" 은 이 문장에 쓰인 것과 같이 단어의 모든 문자가 대문자로 쓰이는 경우에 한해 BCP 14 RFC 2119 [2] 와 RFC 8174 [3] 에 서술된 바와 같이 해석된다.

2. 일반적인 요구사항(General Requirements - GR)

GR-01: 디바이스의 설명은 주요 부품의 식별정보를 포함해야 한다(MUST). 구체적으로는 다음과 같다.:

   a. 제조자, 모델 및 칩셋의 버전
   b. 펌웨어와 기본 OS 의 명칭, 버전, 릴리스 날짜

GR-02: 판매자는 최소한 다음 내용을 서술한 문서를 제공해야 한다(MUST).:

   a. 펌웨어의 기능 또는 OS 의 명칭, 버전, 릴리스 날짜
   b. 디바이스에 구현된 모든 어플리케이션과 서비스의 명칭, 버전, 릴리즈 날짜, 공장 출하시 부팅 스테이터스(factory-boot status)

GR-03: 판매자는 사용하고 있는 모든 오픈소스 소프트웨어의 정보를 제공해야 한다(MUST) :

   a. 사용하고 있는 각 오픈소스 소프트웨어에 관련된 모든 라이센스 정보 목록

b. CPE 시스템에 임베디드된 각 오픈 소스 소프트웨어의 완전한 명칭과 버전

GR-04: 취약성 공개를 위한 연락처 정보 (VR-03)는 CPE 의 그래픽 유저 인터페이스(GUI)의 어딘가(예: 페이지, 탭 등)에 표시되어야 한다(SHOULD).

GR-05: 판매자는 CPE 가 기술지원 기한이 만료되었거나(VR-01 과 VR-02 참조) 펌웨어의 업데이트를 더이상 받을 수 없는 경우(예: 그래픽 유저 인터페이스 등), 사용자에게 (예: 그래픽 유저 인터페이스 등을 통해)정보를 제공해야 한다(SHOULD).

3. 소프트웨어 보안 요구사항(Software Security Requirements - SSR)

SSR-01: 인증정보는 하드 코딩되면 안 된다(MUST NOT). FR-04 와 FR-05 를 참조.

SSR-02: 디바이스에 저장된 민감한 인증정보(예: 비밀번호, 키, 보안 토큰 등)는 적절한 해시화/암호화 알고리듬에 의해 보호되어야 한다(MUST). 암호화 키는 가능한 한 보안상으로 안전한 하드웨어에 저장되어야 한다(SHOULD).

SSR-03: 디바이스에 저장된 일반 데이터는 적절한 암호화로 보호되어야 한다(SHOULD).

SSR-04: 펌웨어 및 시스템 개발에 사용된 소프트웨어와 백도어는 어떠한 것이든 제품의 대량 생산 버전에서 삭제되어야 한다(MUST).

4. 업데이트와 관리 요구사항(Update and Management Requirements - MR)

MR-01: CPE 는 최소한의 적절한 암호화 프로토콜을 사용한 원격 관리를 위한 메커니즘을 구현해야 한다(MUST). 요구되는 프로토콜에 대해서는 부록 I 의 표를 참조.

MR-02: CPE 는 보안상 안전한 원격 업데이트 메커니즘을 구현해야 한다(MUST). 요구되는 프로토콜에 대해서는 부록 I 을 참조.

MR-03: 원격 관리와 관리자 기능, 원격 업데이트 메커니즘은 다음을 지원해야 한다(MUST). :

a. 보안상 안전한 인증
b. 암호화된 접속
c. 특정 소스에 대한 접속 제한(예: 특정 네트워크 영역, 특정한 URL 등)
d. 접속 포트 선택의 자유(예: 디폴트(DEFAULT) 또는 미리 할당된 포트 번호로부터의 포트 번호 변경 지원[17]).

MR-04: 보안상으로 안전한 자동 업데이트의 경우, 그 메커니즘은 소스 레포지토리를 인증하고 검증할 수 있어야 한다(MUST).

MR-05: CPE 는 실제 업데이트가 진행되기 전에(일반적으로 플래시 메모리 상에서) 다운로드된 파일의 통합과 입증 그리고 이것이 해당 디바이스를 위한 것인가(예를 들면 디바이스 설계, 모델, 버전 등)를 확인(Verify)할 수 있는 메커니즘을 구현해야 한다(MUST).

MR-06: 업데이트 프로세스는 현재의 설정을 보존해야 한다(MUST). 판매자는 특정한 설정 변경이 디바이스의 보안을 높이는 경우 현재의 설정을 변경할 수 있다(MAY). 이 경우의 특정한 설정은 명확하게 문서화해야 한다(MUST).

MR-07: 업데이트의 확인에 대하여 CPE 는:

a. 스케줄 베이스의 자동 업데이트를 가져올 수 있도록 정기적인 체크 능력을 보유해야 한다(MUST).
b. 사용자가 업데이트 체크를 시작할 수 있도록 허가해야 한다(MUST).
c. 온디맨드 베이스의 ISP 측 푸시 업데이트를 지원해야 한다(SHOULD).

MR-08: CPE 는 펌웨어 업데이트의 실패의 결과로 인해 사용불능 상태가 되는 것을 방지하기 위한 메커니즘을 구현해야 한다(MUST). 복구 절차는 명확하게 문서화해야 하며(MUST) 하드웨어 내부 부품에 접근할 필요가 없어야 한다(MUST NOT).

5. 기능 요구사항(Functional Requirements - FR)

이 문서는 RFC 7084 [8]에 따른 IPv6 지원이 일반적 구매 요구 문서에 포함되어 있음을 가정하여 작성되었다.

CPE 에서 지원되어야 하거나 CPE 에서 제거되어야 하는 기능은 다음과 같다.:

FR-01: CPE 는 민감한 정보 제시를 허락하거나 증폭 공격(예: Telnet, FTP, SOCKS, CHARGEN, SNMP 등)을 실행할 수 있도록 하는 디폴트 상태의 WAN(WAN BY DEFAULT) 서비스를 유효화 해서는 안 된다(MUST NOT).

FR-02: CPE 는 원격 업데이트와 원격 관리 기능을 이 문서의 업데이트와 관리 요구사항(Update and Management Requirements - MR) 항목에서 서술된 바와 같이 구현해야 한다(MUST).

FR-03: LAN/WLAN 상에서 CPE 로 행해지는 모든 엔드유저 관리의 통신은 인증되어야 하고(MUST)[6]. 암호화되어야 한다(SHOULD).

FR-04: 모든 인증정보(예: 비밀번호)는 마스터 관리자(root)를 포함해 변경 가능해야 한다(MUST). 사용자 식별정보(예: 사용자명)는 변경 가능해야 한다(SHOULD).

FR-05: 관리자 인터페이스에 접근하기 위한 비밀번호는:

a. 초기 비밀번호는 각각의 디바이스가 개별적으로 유니크해야 하며(MUST) 패킷 캡처 또는 그와 비슷한 관찰(예: MAC 어드레스)을 통해 유추할 수 있으면 안 된다(MUST NOT).
b. 비밀번호가 변경되거나 리셋되었을 때는 언제라도 그 비밀번호가 null(예: 값이 없음, 공백) 또는 사용자명이어서는 안 되며(MUST NOT), 비밀번호의 복잡성에 관한 베스트 프랙티스를 따라야 한다(MUST).

[6] CPE 는 심플한 유저명/비밀번호보다 높은 보안성을 가진 인증 메커니즘을 지원해야 한다.

FR-06: 펌웨어 제품은 시스템 또는 그 데이터에 접근하기 위한 비문서화된 메커니즘은 어떠한 것도 보유해서는 안 된다(MUST NOT).

FR-07: 디바이스는 데이터를 판매자 또는 서드파티에 보내기 위한 비문서화된 통신 메커니즘은 어떠한 것도 보유해서는 안 된다(MUST NOT). 판매자나 서드파티에게 보내지는 모든 통신과 데이터는 명확하게 문서화되어야 한다(MUST)[7].

FR-08: 인증된 엔드유저는 그래픽 유저 인터페이스를 통해 다음이 가능해야 한다(MUST).:

a. 사용자 고유 설정의 적절한 변경(예: WiFi 네트워크명, 방화벽/전송 규칙 등).
b. 디바이스의 조작 및 관리에 불필요한 모든 서비스의 무효화.

FR-09: CPE 의 LAN/WAN 인터페이스 상에서의 사용자를 위한 서비스 조작을 유효화할 경우, DNS, NTP, SSDP, UPnP 및 증폭 공격에 사용될 가능성이 있는 프로토콜을 이용하는 특정 서비스는 WAN/인터넷에 접속할 수 있어서는 안 된다(MUST NOT).

FR-10: 서비스/에이전트를 모니터링 및 관리하기 위해서는:

a. 값의 설정과 정보/민감한 데이터의 취득을 위한 적절한 인증 메커니즘 설정이 요구된다(MUST).
b. WAN 인터페이스로부터의 액세스는 반드시 인증을 사용해야 하며(MUST) 특정 소스(예: 특정 네트워크 영역 또는 주소)를 제한해야 한다(MUST).

FR-11: 디바이스는 현 버전에서의 암호 스위트와 키 사이즈를 고려하여 안전한 파라미터 선택을 허용하는 오픈 스탠더드 베이스의 암호화 방법을 구현해야 한다(MUST).

FR-12: 디바이스 인증에 사용되는 키 및 전자증명서의 생성을 위한 암호화 서비스 또는 애플리케이션은 각 개별 디바이스별로 키 및 전자증명서를 생성해야 한다(MUST). 예를 들어 프라이빗키는 다른 디바이스와 결코 공유되어서는 안 된다(MUST NOT).

FR-13: CPE 는 네트워크 타임 프로토콜(Network Time Protocol - NTP)와 같은 중앙 집중식 타임 프로토콜을 통해 시간 동기화를 지원해야 한다(MUST). 이를 위해서는 NTP 를 위한 클라이언트 소프트웨어가 요구된다. CPE 는 NTP 서버를 위한 하드코딩된 설정을 가져서는 안 되며(MUST NOT) 판매자가 사용을 허가받지 못한 서버를 디폴트로(BY DEFAULT) 사용해서는 안 된다(MUST NOT).

FR-14: CPE 는 RFC 6092 "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service"[6] 를 지원해야 한다(SHOULD). RFC 6092 와 이 문서에 모순이 있는 경우, 이 문서의 요구사항이 우선된다.

FR-15: CPE 는 BCP 38, RFC 2827 [12] 에 따라 IPv4 와 IPv6 양쪽 모두의 안티스푸핑 필터를 지원해야 한다(MUST). 이것은 디폴트에 의해(BY DEFAULT) 유효화 설정이 가능한

[7] 많은 국가/지역에서 데이터 보호에 대한 입법은 개인 데이터 처리에 대해 상세하고 명확하게 문서화된 특별한 사항을 요구하는 경우가 있다.

옵션이어야 한다(MUST). 소스 IP 주소의 검증에 사용되는 기술의 결정은 이 문서의 범위에 포함되지 않는다.

FR-16: CPE 는 특별한 목적을 가진 IP 주소에 대한 패킷 필터링을 지원해야 한다(SHOULD). RFC 6890 [13] 과 RFC 8190 [14]에 따라, "Globally Reachable" FALSE AND "Forwardable" FALSE 인 주소는 필터링되어야 한다(SHOULD). 이 경우 CPE 는 "IANA IPv4 Special-Purpose Address Registry" [15] 와 "IANA IPv6 Special-Purpose Address Registry" [16]에 서술된 바와 같이 IANA (Internet Assigned Numbers Authority) 에 의해 유지되고 있는 기재내용에 따라 IPv4 와 IPv6 를 포함해 설정할 수 있어야 한다(SHOULD).

FR-17: CPE 는 오픈 리졸버로서 기능해서는 안 된다(MUST NOT).:

a. WAN 포트에서 수신해 CPE 본체에 향하는 DNS 쿼리는 WAN 포트에서 어떠한 경우에도 허가되거나 응답해서는 안 된다(MUST NOT).

b. WAN 포트에서 수신해 LAN 포트로의 전송을 의도하는 DNS 쿼리는 CPE 설정에 명시적인 규칙이 존재하는 경우에만 허용될 수 있다(MAY). (예: 전송 규칙, 방화벽 규칙 등)[8].

c. CPE 가 로컬 DNS 서버를 실행하는 경우, 아웃바운드 DNS 쿼리가 DNSSEC 검증을 실행하도록 설정해야 한다(SHOULD).

d. CPE 가 로컬 DNS 서버를 실행하지 않는 경우, DNSSEC 검증 마킹이 존재한다면 다른 서버에 DNS 쿼리를 전송하는 대신 DNS 에서 DNSSEC 검증 마킹을 삭제해서는 안 된다(MUST NOT).

FR-18: CPE 가 WiFi 를 제공하는 경우:

a. 적절한 암호화를 수반하는 보안 메커니즘을 구현해야 한다(MUST).

b. 최신 버전의 Wi-Fi Protected Access (WPA)®의 보안 기능 명세를 지원해야 한다 (SHOULD).

FR-19: 비밀번호는 어떠한 관리 인터페이스에서도 디폴트상(BY DEFAULT) 클리어 텍스트로 보여져서는 안 된다(MUST NOT). 비밀번호는 사용자의 요청이 있는 경우에만 눈으로 볼 수 있다(MAY).

FR-20: 디바이스 설정은 출력물에서 민감한 정보(예: 비밀번호, SNMP 등 Community 문자열)가 지워지거나 마스킹된 상태로 클리어 텍스트 포맷(ASCII 또는 UTF-8)으로 다운로드할 수 있는 방법이 존재해야 한다(SHOULD).

[8] CPE 는 사용자가 LAN 안에서 DNS 서버를 호스팅하는 것을 방해해서는 안 된다. 이는 포워딩/방화벽 규칙에 대해서도 마찬가지로 적용된다.

6. 초기 설정 요구사항(Initial Configuration Requirements - IR)

디바이스는 다음과 같은 공장 출하시의 초기 디폴트 설정을 가져야 한다(MUST):

IR-01: CPE 는 사용을 허용보다는 제한하는 방향으로 설정되어야 한다(MUST). 초기 설정 프로세스(bootstrapping)을 위한 필요하지 않은 모든 서비스(예: 서비스 타입 프로세스)는 사용 불가능한 상태여야 한다(MUST). 특히 (구현되어 있다면) SSDP, SNMP, UPnP, SOCKS, SMB, 대역 테스트(ergo 에 임베디드된 iperf 나 다른 것들)이 그렇다. 추가적으로, 엄격한 운용을 위한 또는 보안상 안전한 모드를 위한 서비스는 사용 가능한 상태이거나 사용되고 있는 상태여야 한다(SHOULD).

IR-02: DNS 서버 주소(리졸버 주소)에 관련된 파라미터는 설정이 없어야 하며(MUST), (구현되어 있다면) DNS 릴레이 옵션이 사용 불가능한 상태여야 한다(MUST).

IR-03: 포트 포워딩 또는 DMZ 호스트 옵션은 가능하다면 디폴트로(BY DEFAULT) 사용 불가능한 상태여야 한다(MUST).

IR-04: 그래픽 또는 커맨드라인의 관리자 인터페이스에 접근하기 위한 초기 비밀번호는 각각의 개별 디바이스별로 고유한 것이어야 하며(MUST) 디바이스의 라벨에서 눈으로 볼 수 있어야 한다(MUST).

IR-05: WiFi 가 제공되는 경우, WiFi 네트워크는 WiFi SSID 와 다른(NOT) 고유한 초기 비밀번호를 가져야 하며(MUST) 이 초기 비밀번호는 디바이스의 라벨에서 눈으로 볼 수 있어야 한다(MUST). 이 비밀번호는 디폴트(DEFAULT) 관리자 비밀번호와는 다른 것이어야 한다(SHOULD).

IR-06: WiFi 가 제공되는 경우, WiFi Service Set Identifier(SSID) 의 디폴트(DEFAULT) 값은 판매자의 이름 또는 제품의 모델명과 관련되어서는 안 되며(MUST NOT), 커스터마이즈 가능해야 한다(MUST). ISP 의 디폴트(DEFAULT) 값 커스터마이즈에 대해서는 부록 I에서 참고 가능하다[9].

IR-07: SSH 서비스의 경우, 서버의 키페어는 공장에서 사전 생성되지 않아야 한다(MUST NOT) . 키는 최초 서비스 초기화 및 부팅 후에 생성되어야 하며 디바이스의 모든 공장 초기화 후에는 새로운 키를 생성해야 한다(MUST). 생성된 키페어는 서비스 적용시 보안상 충분히 안전하다고 생각되는 수준의 보안성을 제공해야 한다.

IR-08: 안티스푸핑 필터 [FR-15] 는 디폴트로(DEFAULT) 유효화되어야 한다(MUST).

IR-09: IPv6 이행 메커니즘, 터널, VPN 및 유사한 서비스는 디폴트로(BY DEFAULT) 사용 불가능한 상태여야 한다(MUST).

[9] ISP 가 SSID 이름의 디폴트(BY DEFAULT) 설정 방식(예: 모든 디바이스에 하나의 이름을 두거나 각각의 디바이스 별로 고유한 이름을 설정하는 등)을 결정할 경우, ISP 는 SSID 이름의 설정 방식에 대해 설명할 필요가 있다. 그렇지 않다면 판매자는 디폴트(DEFAULT)를 선택할 수 있다.

7. 판매자 요구사항(Vendor Requirements - VR)

판매자는:

VR-01: 제품 판매 기간이 끝난 후에도 보안 취약점에 대해서는 수정할 수 있어야 함을 충분히 고려하여 제품 지원 정책을 명확히 해야 한다(MUST).

VR-02: 디바이스가 판매되는 동안 최소한의 보안 취약점을 수정할 수 있어야 한다(MUST). 판매자는 제품 판매 기간이 끝난 뒤 3 년간 보안 취약점 수정 패치를 제공해야 한다(SHOULD).

VR-03: 제품에서 발견된 보안 취약점을 ISP 고객, 엔드유저, 서드파티(연구자와 같은)에게 보고할 수 있는 의사소통 채널/연락 창구를 포함해 공동으로 보안 취약점을 공개할 수 있는 능력을 가져야 한다(MUST). 제품의 보안 이슈 대응팀(Product Security Incident Response Team - PSIRT)이 존재하는 것이 이상적이다(SHOULD).

VR-04: 사전 등록이나 계정이 필요없는 공개적 지원 채널을 가져야 한다(MUST). 영어 웹사이트에는 최소한 다음 내용이 있어야 한다.:

a. 현재 존재하는 보안 취약점과 그 완화 방법, 제품의 해당 보안 관련 패치의 정보 제공.
b. 보안 관련 패치 및 제품을 위한 펌웨어 또는 소프트웨어의 새로운 버전의 제공.
c. 디바이스의 설정, 업데이트, 보안을 위한 매뉴얼 및 기타 자료의 제공.

8. 약어 목록

BCOP: Best Current Operational Practices

BBF: Broadband Forum

CE: Customer Edge Router

CPE: Customer Premises Equipment

CWMP: CPE WAN (Wide Area Network) Management Protocol

IANA: Internet Assigned Numbers Authority

ISP: Internet Service Provider

PSIRT: Product Security Incident Response Team

RG: Residential Gateway

SSID: Service Set Identifier

WLAN: Wireless LAN (Local Area Network)

9. 감사의 말

이 문서의 작성 시작부터 공개에 이르기까지 Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG)의 많은 사람들이 공헌하였다.

이 문서의 작성자들은 문서 작성에 많은 도움과 제안, 상세한 리뷰를 제공해 준 공헌자들에게 감사의 말을 전한다. 공헌자들의 이름은 다음과 같다(알파벳 순).:

Nicolas Antoniello, John Brown, Dennis Dayman, Carmen Denis, Yuri Ferreira, Alexandre Giovaneli, Steve Goeringer, Cristine Hoepers, Markus Lintula, Jason Livingood, Art Manion, Jordi Palet Martínez, Roney Medeiros, Luciano Minuchin, Eduardo Barasal Morales, Massimiliano Pala, Ricardo Patara, Nathalia Sautchuk Patrício, Fernando Quintero, Marcelo Batista Sarmento, Joe St Sauver, Klaus Steding-Jessen, Italo Valcy, Severin Walker, Ariel Weher, Gilberto Zorello, Jan Žorž.

특히 다음 사람들에게 감사의 말을 전한다.:

- Lucimara Desiderá (LAC-AAWG 설립의 공동 의장, 저자/편집자)
- Christian O'Flaherty (LAC-AAWG 설립의 공동 의장)
- 문서화 및 리뷰 프로세스를 지원한 LACNOG BCOP 워킹 그룹 커뮤니티와 의장
- 대면 회의를 위한 인프라를 제공한 라틴아메리카의
- The LACNIC WARP (Warning Advice and Reporting Point)와 Caribbean Internet Address Registry (LACNIC)
- LAC-AAWG 의 초안을 지원하고 테크니컬 리뷰를 담당한 The Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

10. 인용 정보

[1] Abuse of Customer Premise Equipment and Recommended Actions
https://resources.sei.cmu.edu/asset_files/WhitePaper/2014_019_001_312679.pdf

[2] Key words for use in RFCs to Indicate Requirement Levels, BCP 14, RFC 2119
http://www.rfc-editor.org/info/rfc2119

[3] Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words, RFC 8174
https://tools.ietf.org/html/rfc8174

[4] Internet Security Glossary, Version 2, RFC 4949
https://tools.ietf.org/html/rfc4949

[5] Common Security Requirements for IP-Based MSO-Provided CPE - Version I01
https://apps.cablelabs.com/specification/common-security-requirements-for-ip-based-mso-provided-cpe

[6] Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service, RFC 6092
https://tools.ietf.org/html/rfc6092

[7] Data-Over-Cable Service Interface Specifications DOCSIS® 3.1, Security Specification, CM-SP-SECv3.1-I07-170111
https://apps.cablelabs.com/specification/CM-SP-SECv3.1

[8] Basic Requirements for IPv6 Customer Edge Routers, RFC 7084
https://tools.ietf.org/html/rfc7084

[9] Functional Requirements for Broadband Residential Gateway Devices, TR-124 Issue 5
https://www.broadband-forum.org/technical/download/TR-124_Issue-5.pdf

[10] CPE WAN Management Protocol, TR-069 Issue 1 Amendment 6
https://www.broadband-forum.org/technical/download/TR-069.pdf

[11] IPv4 and IPv6 eRouter Specification CM-SP-eRouter-I19-160923
https://apps.cablelabs.com/specification/ipv4-and-ipv6-erouter-specification/

[12] Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, BCP 38, RFC 2827
https://tools.ietf.org/html/rfc2827

[13] Special-Purpose IP Address Registries, BCP 153, RFC 6890
https://tools.ietf.org/html/rfc6890

[14] Updates to the Special-Purpose IP Address Registries, BCP 153, RFC 8190
https://tools.ietf.org/html/rfc8190

[15] IANA IPv4 Special-Purpose Address Registry
https://www.iana.org/assignments/iana-ipv4-special-registry

[16] IANA IPv6 Special-Purpose Address Registry
https://www.iana.org/assignments/iana-ipv6-special-registry

[17] Service Name and Transport Protocol Port Number Registry
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

[18] Addressing the challenge of IP spoofing
https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AntiSpoofing-20150909-en-2.pdf

[19] ISO/IEC 29147:2014 Information technology - Security techniques - Vulnerability disclosure
https://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip

[20] BSI TR-03148: Secure Broadband Router
Requirements for a secure Broadband Router Version: 1.0
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=2

부록 1 - 요구사항 표

다음 표는 이 문서에서 제공하는 요구사항의 세트를 요약하고 있으며, ISP 와 같은 조직이 RFP 를 준비하는 것과 그들이 판매자에게 원하는 요구사항을 명확히 함에 있어 도움을 주는 것에 의미를 두고 있다.

몇몇 필드는 의무적 요구사항을 고려한 추천 선택지로 채워져 있다. 그러나 요구사항의 많은 부분은 주어진 설정을 그대로 사용할 것인지 아닌지, 디폴트(DEFAULT) 설정을 새롭게 정의할 것인지에 대해 조직의 결정을 요구한다.

이 문서에 기재된 사항은 보안 요구사항의 최소한의 세트이며 그 설정을 낮은 수준(예: 필수 사항에서 추천 또는 선택적 구현까지)으로 내리지 않을 것을 강력하게 추천한다. 가능한 한 언제든 가장 엄격한 설정을 선택할 것을 권장한다.

일반 요구사항(General Requirements - GR)		
요구사항 (Requirement)	**M 필수(Mandatory)** **R 추천(Recommended)** **O 옵션(Optional)**	**디폴트 설정(Default configuration)**
GR-01	M	
GR-02	M	
GR-03	M	
GR-04	R	보안상 취약성 정보 공개에 대한 연락처가 그래픽 유저 인터페이스 상에 존재할 것
GR-05	R	현재의 업데이트 상황(Current status of updates)
소프트웨어 보안 요구사항(Software Security Requirements - SR)		
요구사항 (Requirement)	**M 필수(Mandatory)** **R 추천(Recommended)** **O 옵션(Optional)**	**디폴트 설정(Default configuration)**
SSR-01	M	
SSR-02	M	민감한 정보를 보호할 것 Sensitive data protected
SSR-03	R	
SSR-04	M	소프트웨어 개발 도구 및 백도어는 삭제할 것

업데이트와 관리 요구사항 (Update and Management Requirements - MR)		
요구사항 (Requirement)	**M 필수(Mandatory) R 추천(Recommended) O 옵션(Optional**	**디폴트 설정(Default configuration)**
MR-01	M (a)	(a)
MR-02	M (b)	(b)
MR-03	a. M b. M c. M d. M	(c)
MR-04	M	
MR-05	M	
MR-06	M	
MR-07	a. M b. M c. R	
MR-08	M	
기능 요구사항(Functional Requirements - FR)		
요구사항 (Requirement)	**M 필수(Mandatory) R 추천(Recommended) O 옵션(Optional)**	**디폴트 설정(Default configuration)**
FR-01	M	Telnet, FTP, SOCKS, CHARGEN, SNMP 무효화
FR-02	M	(c)
FR-03	인증 필수(MUST), 암호화 추천(RECOMMENDED)	
FR-04	M	
FR-05	a. M b. M	각각의 개별 디바이스가 고유한 초기 비밀번호를 가질 것
FR-06	M	
FR-07	M	

FR-08	a. M b. M	
FR-09	M	DNS, NTP, SSDP, UPnP 가 WAN 에서 접속 불가능 할 것
FR-10	a. M b. M	(d)
FR-11	M	
FR-12	M	
FR-13	M	NTP 클라이언트만 해당. 하드코딩 설정하지 않을 것
FR-14	R	
FR-15	M	안티스푸핑 필터(Anti-spoofing filtering) 유효화
FR-16	R	설정하지 않을 것 (e)
FR-17	a. M b. R c. R d. M	b. 전송 규칙을 유효화하지 않을 것
FR-18	a. M b. R	적절한 암호화를 유효화할 것
FR-19	M	
FR-20	R	

초기 설정 요구사항(Initial Configuration Requirements - IR)

요구사항 (Requirement)	**M 필수(Mandatory) R 추천(Recommended) O 옵션(Optional)**	**디폴트 설정(Default configuration)**
IR-01	M	SSDP, SNMP, UPnP, SOCKS, SMB, 대역 테스트 무효화
IR-02	M	사전 정의된 DNS 주소가 없을 것, DNS 릴레이는 무효화할 것
IR-03	M	무효화
IR-04	M	(f)

IR-05	M	(f)
IR-06	M	(g)
IR-07	M	사전 생성된 SSH 가 없을 것
IR-08	M	유효화
IR-09	M	통과 메커니즘, 터널, VPN 의 무효화
판매자 요구사항(Vendor Requirements - VR)		
요구사항 (Requirement)	**M 필수(Mandatory) R 추천(Recommended) O 옵션(Optional)**	**디폴트 설정(Default configuration)**
VR-01	M	
VR-02	M	
VR-03	M	
VR-04	M	

(a) ISP 는 디바이스를 원격 관리할 수 있는 능력(예: 설정 능력)을 가져야 한다. 공급자(케이블, 광케이블, xDSL)에 의해 사용된 기술에 따라, 해당 산업은 이미 특정한 프로토콜을 가지고 있을 것이다. 이 항목에서 ISP 는 디바이스에 필요한 기술(예: 브로드밴드를 위한 BBF TR-069 CWMP)에 따라 프로토콜을 선택할 필요가 있으며 이를 디폴트로(BY DEFAULT) 유효화 또는 필요한 초기 설정을 해야 한다. 복수의 프로토콜이 지원되는 경우, 조직은 그 모두를 이 항목에 포함시킬 필요가 있다.

(b) ISP 는 디바이스를 원격으로 업데이트할 능력(주로 펌웨어)을 가져야 한다. 공급자(케이블, 광케이블, xDSL)에 의해 사용된 기술에 따라, 해당 산업은 이미 특정한 프로토콜을 가지고 있을 것이다. 이 항목에서 ISP 는 디바이스에 필요한 기술(예: 브로드밴드를 위한 BBF TR-069 CWMP)에 따라 프로토콜을 선택할 필요가 있으며 이를 디폴트로(BY DEFAULT) 유효화 또는 필요한 초기 설정을 해야 한다. 복수의 프로토콜이 지원되는 경우, 조직은 그 모두를 이 항목에 포함시킬 필요가 있다.

(c) CPE 와 그 관리/업데이트 서버의 트랜젝션에 있어 액세스 컨트롤, 기밀 유지 및 통합 체크를 위한 최소한의 메커니즘을 사용하지 않는 것은 종종 공급자의 인프라와 타협한 결과일 수 있다. 이때 모든 액세스는 암호화된 접속(예: TLS/HTTPS)에서 이루어질 것, 모든 디바이스에 사전 설정된 공통된 하나의 사용자명/비밀번호가 아닌 것으로 인증할 것, 특정한 소스(예: 선택된 네트워크 영역, 특정 URL 등)에 대한 액세스를 규제할 것을 강력하게 권장한다.

(d) ISP 가 모니터링 및 관리 서비스/에이전트를 디폴트로(BY DEFAULT)로 유효화하기를 원할 경우, 인증과 네트워크 액세스 규제를 위한 적절한 파라미터를 제공해야 한다.

(e) ISP 가 CPE 에서 직접적으로 Special-Purpose IP 주소에 대한 필터링을 구현하기를 원할 경우, 디폴트로(BY DEFAULT) 필터링될 프레픽스의 목록을 제공할 수 있다. 그렇지 않다면 디폴트(DEFAULT) 설정은 미설정(unconfigured)이며 CPE 는 특정 프레픽스에 대해 어떠한 필터도 적용하지 않는다.

(f) ISP 가 초기 비밀번호를 커스터마이즈하기 원할 경우 비밀번호 선택 프로세스를 판매자에게 알릴 필요가 있다. 그렇지 않은 경우 판매자는 디폴트(DEFAULT) 로써 랜덤한 고유한 값을 설정할 수 있다.

(g) ISP 가 WiFi 네트워크명을 커스터마이즈하기 원할 경우 WiFi 식별자(SSID)의 설정 방법을 알릴 필요가 있다. 그렇지 않은 경우 판매자는 디폴트(DEFAULT) 값을 선택할 수 있다. .

이 문서는 산업의 발전과 공헌을 위해 또한 LACNOG 와 M³AAWG 집필진에게 경의를 표하기 위해 Mihyon Hirano, Qualitia Co., Ltd, JPAAWG 가 한국어로 번역하였습니다.
https://www.qualitia.co.jp/

공개된 다른 모든 문서와 같이 이 문서의 업데이트에 대해서는 M³AAWG 웹사이트 (www.m3aawg.org) 또는 LACNOG 웹사이트 (www.lacnog.net) 에서 확인하실 수 있습니다.

M3AAWG127-LACNOG-Korean