M2M 제휴단말 개발보안 프로세스 및 보안점검 항목

- 주요 공지 안내
- 제휴단말 개발보안 프로세스 및 보안점검 항목
- 댓글 질문 이벤트

제3회 B2B 무선 사업 파트너 웨비나

2022. 6. 29

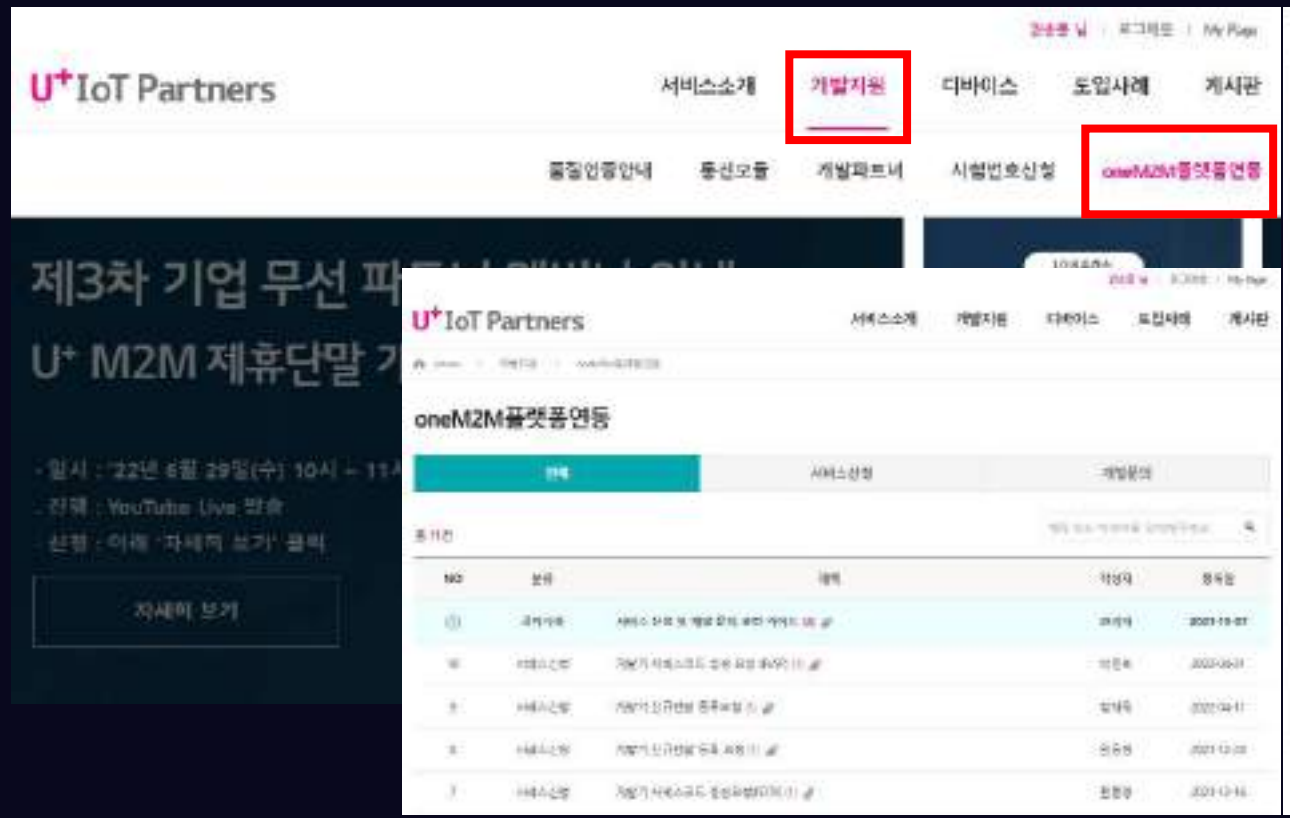
주요 공지 안내 (1/3)

oneM2M 플랫폼 연동 게시판 이용안내

01 oneM2M(LwM2M) 플랫폼 연동 서비스 신청 및 기술지원 문의 게시판 위치 (개발지원 > oneM2M플랫폼연동)　※ Q&A커뮤니티 게시판 아님

02 oneM2M(LwM2M) 개발팀 직접 답변 (평균 답변 소요시간 영업일 기준 1~2일)

03 로그인 후 oneM2M(LwM2M) 플랫폼 연동 게시판 이동 시 기업회원 동일 소속 내용만 보임 (타사 정보 확인 불가)　※ 관리자는 별도 시스템 확인





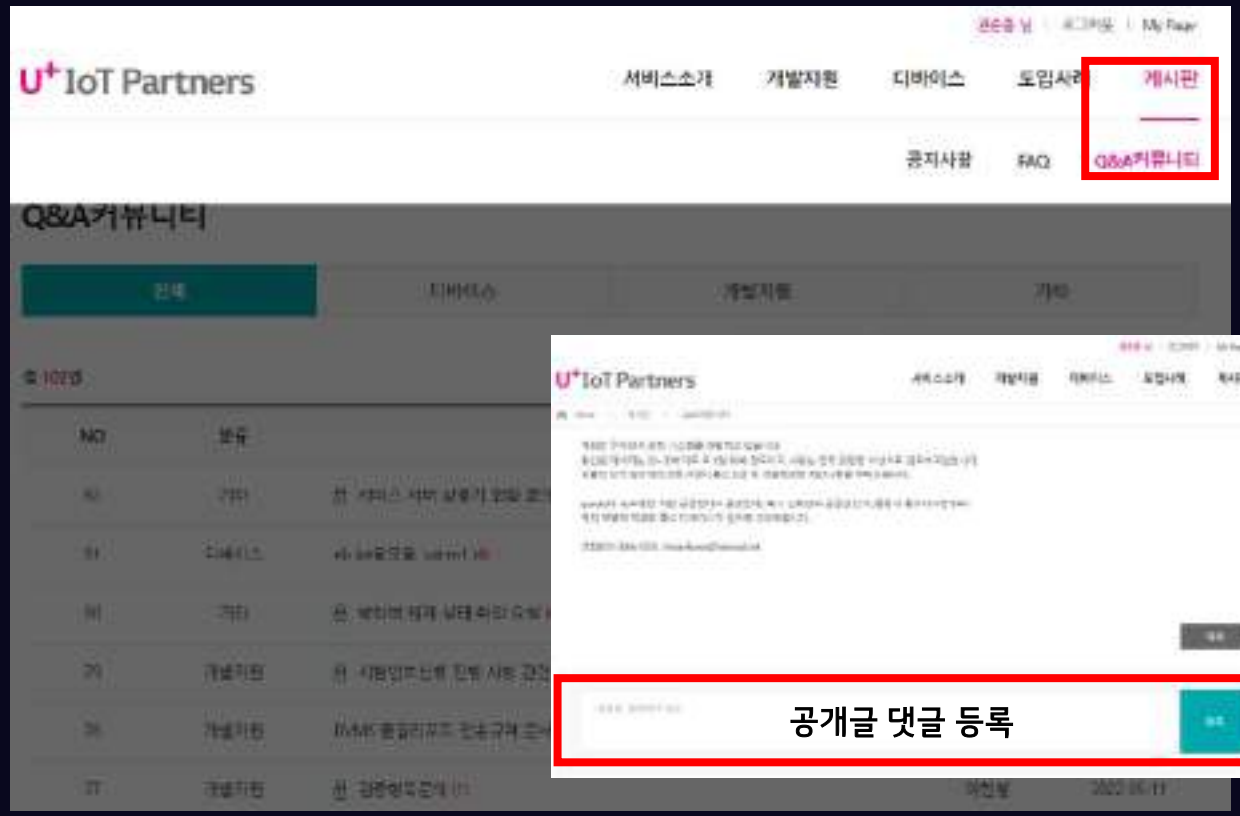
주요 공지 안내 (2/3)

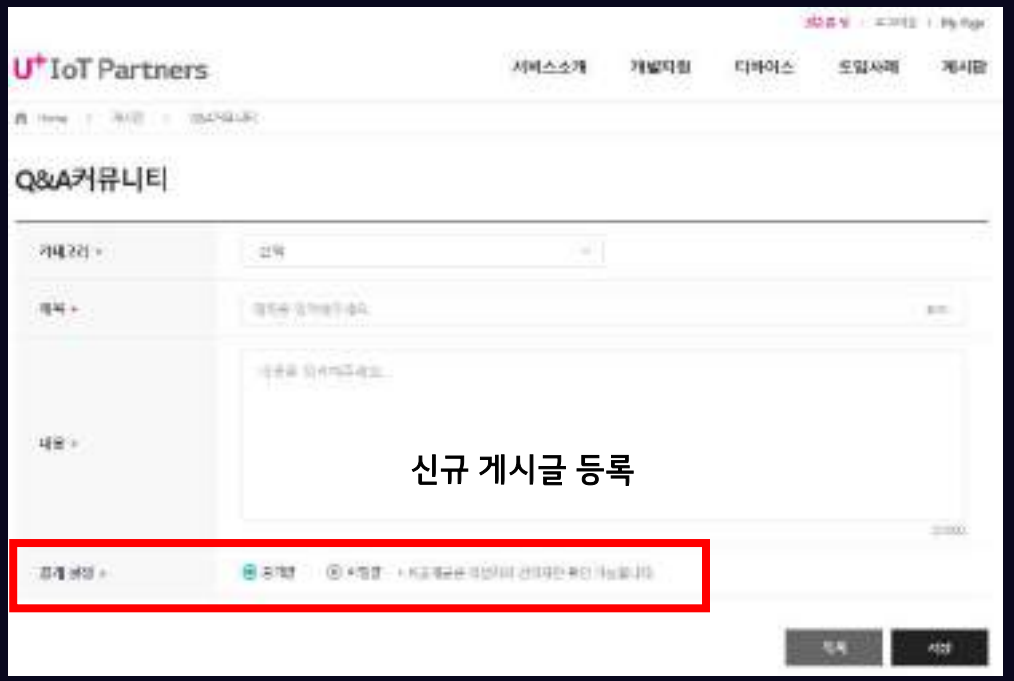
Q&A커뮤니티 게시판 이용안내

01 oneM2M 플랫폼 연동 개발지원은 제외한 서비스, 요금제, 제품정보, U+IoT Partners 등 업무 관련 문의 게시판 위치 (게시판 > Q&A커뮤니티)

02 공개글인 경우 누구나 댓글 등록 가능 (파트너사간 노하우 공유 및 지식 창고 활용)

03 민감한 내용인 경우 게시글을 비밀글로 신규 등록 ※ 관리자만 조회/답변 가능





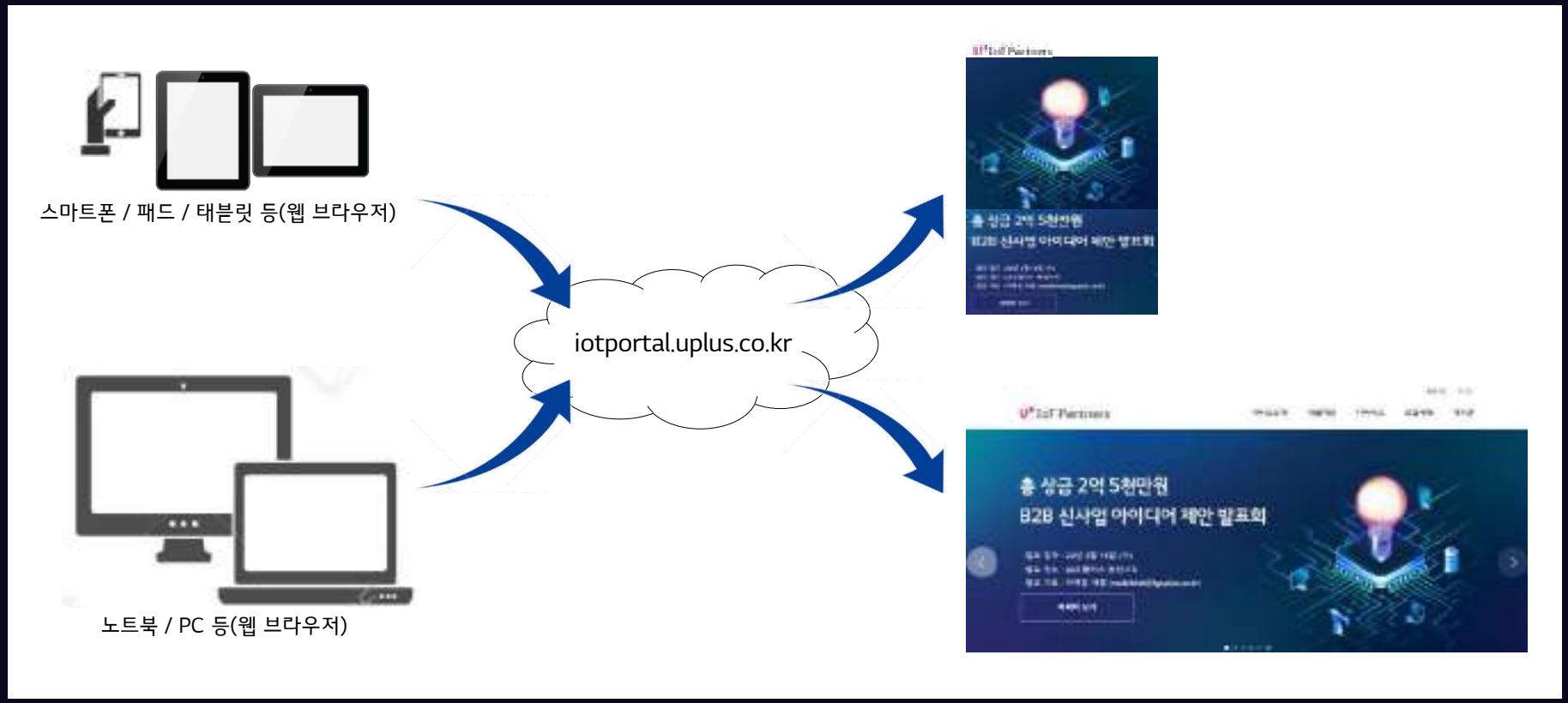
주요 공지 안내 (3/3)

U+ IoT Partners 고도화 ('22년 말 예정)

01 현재 PC 최적화 화면은 MOBILE 기기에서도 원활히 이용할 수 있도록 반응형 웹으로 수정 개발

02 파트너 업무 지원 부분에서 건의 및 칭찬, 좋아요/싫어요 의사 표현을 통해 파트너 & 파트너, 파트너 & LG유플러스 파트너쉽 강화

03 간편 로그인, 공지사항 외부 공유 기능, 공지사항 첨부파일 제한 해제, oneM2M 문의글 읽음표시 기능 등을 통해 이용 편의성 제고



M2M 제휴단말 개발보안 프로세스 및 보안점검 항목

금일 웨비나 내용

2022년 6월 29일 (수)		내용	발표자
1시간	10:00 ~ 10:05 (05')	금일 웨비나 진행 및 주요 공지 안내	 권순홍 님  이권철 님  문용석 님
	10:05 ~ 10:50 (45')	1. 보안사고 사례 2. 관련 법령 3. U+ 개발보안 프로세스 4. 보안점검 항목 및 자가진단 방법 4-1. 인증 4-2. 암호 4-3. 데이터 보호 4-4. 플랫폼 보호 4-5. 물리적 보호 5. 끝맺음	
	10:50 ~ 11:00 (10')	댓글 질문 이벤트	

M2M 제휴단말 개발보안 프로세스 및 보안점검 항목

시작하기 전에...

기업부문 단말 DVMS 등록시 첨부자료

※ DVMS 내에 샘플문서 다운가능 (2021.04.12~)

▶ 기업 디바이스별 사업형태 3가지 유형

a) '제휴형(자급/망제공) 사업형태' 검증시 ①~⑧ (*필수자료)

b) '자사주도형 사업형태' 검증시 ①~⑩ 모두필요 (⑨,⑩ 검증간 접수가능) (자사주도형 = 자사가 단말 매입하여 단말 및 시장품질을 책임지는 경우)

c) '신규모듈' 검증시(망정합 검증) ②③④⑤⑧ (통신칩셋 OnBoard(Built-in) 단말경우 ①~⑧ 필요.)

요청자료	설명	비고
① 품질센터 검토요청서	최종 고객요구사항 있을시 본 문서내 기재 필요	※샘플문서 참조
② 제품 규격서	기능정의서, Hw/Sw규격서 (예. 제품 설명서)	▷제조사 양식
③ 제조사 개발시험 결과서	SW검증(FW) : 시험절차서, 기능별TC, 검증Tool HW검증 : HW기능확인절차서, 검증Tool 및 JIG , 제조사 시험결과서	▷제조사에서 단말개발시 시험한 절차서 요청 (제조사 양식) ▷제휴형 단말 경우 'HW검증'은 인증/시험결과 확인으로 준용
④ KC인증 (+ 기타인증)	단말에 해당되는 법적필수 KC인증 필요 (예. 방송통신기자재,전기안전 등) ① 단말별 필요인증 일체 (예. 방수방진, 방폭, WiFi 등) ② 2차배터리,어댑터 등 부속품도 KC인증 필요	▷해당 단말 필수인증 확인시 질의답변으로 확인가능 (e나라표준인증>1381인증표준(www.1381call.kr 게시판문의))
⑤ RF성능 시험결과	당사시험 (OTA/RCT)시험 또는 NIPA 시험결과 인정 ① LTE,5G 단말/모듈은 당사에서 시험가능 (NIPA시험결과 제출시 준용) ② NB/M1 단말/모듈은 NIPA 시험결과 필요	▷NIPA 무선시험소 담당자 (김동욱 수석 d326@nipa.kr)
⑥ 입고전 검토 리스트	당사규격에 맞는 HW/기능 규격 적용 필요 (문서내 규격 및 체크사항 확인 가능)	※샘플문서 참조
⑦ NW시나리오	당사규격에 맞는 NW품질리포트 적용 필요	※샘플문서 참조 (NW사업기술팀 검토 결과 필요)
⑧ 보안점검(U+)	보안 리스크 대비 체크리스트 검토	▷사업팀 담당자가 진행 (사업 담당자 → 서비스보호팀(이권철님)) ※제휴형 단말경우 체크리스트 제출 및 담당자 검토의견 필요
⑨ 품질관리 특수조건	출시전후 단말 품질리스크 대비 - 업체 물품구매 계약시 부속계약 필요	(자사주도형) 날인 필요 (사업 담당자) ※마당 '전사 규정/지침' 참조 – 수정 필요시 협의후 법무검토 필요
⑩ PL보험	시장품질 리스크 대비	(자사주도형) 가입 필요 (협력업체)
※ 검증 샘플	검증 입고전 담당자 협의후 진행 (자사주도형 단말경우 별도 협의필요) ① 기능검증 샘플(5) : 해지(1),정지(1),에이징(3) ② RF시험 샘플(4) : RCT(2), OTA(2) ③ 망정합 검증 샘플(4) : 프로토콜, 필드테스트	-무선단말 HW/기능검증 : 권용훈님 / 최철호님 -유선단말 HW/기능검증 : 차진 님 -망정합 검증(통신모듈) : 이기훈님 ※ 자사주도형 단말 검증시 샘플수량 사전 협의 필요
※ 개발검증 요청서	당사 개발팀 검증시 개발팀 담당자에게 전달 필요 (예. 신규모듈, 당사 개발인력 투입 시)	※문의 : 송치우 님 (선행검토 DVMS접수시 개발팀 담당자 추가)

M2M 제휴단말 개발보안 프로세스 및 보안점검 항목

시작하기 전에...

전략단말

U+ 개발 및 관리 디바이스

(U+ 공급 및 유지보수 진행 U+ 주도형 디바이스)

VS

제휴단말

U+ 망만 이용하는 디바이스

(파트너사 자체 개발, 유지보수 직접 수행 디바이스)

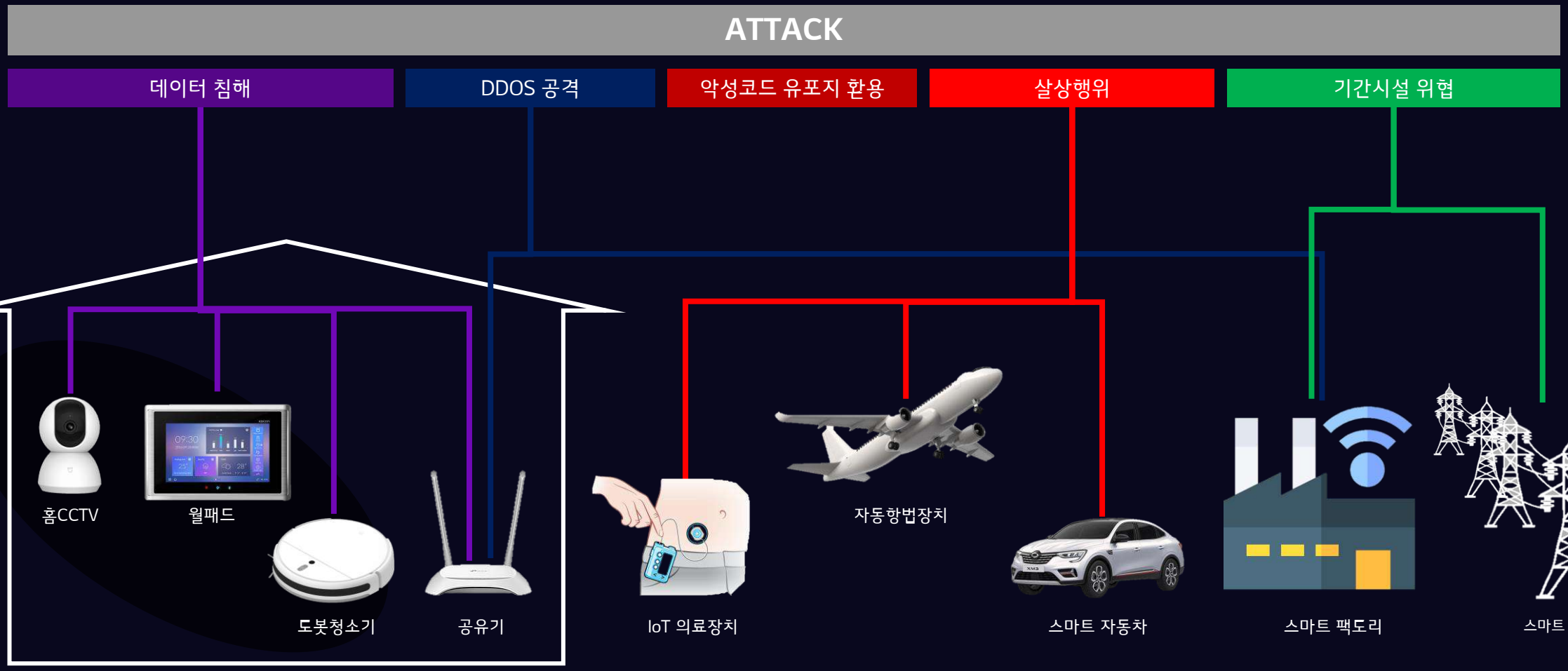
품질 검증 = DVT 개발검증시험 (Development Verification Test) **망 정합성 검증** + CVT 고객검증시험 (Commercial/Customer Verification Test) **기능 검증** + **RF 검증**

제휴단말 품질검증 (U+ 품질검증 통신모듈 사용 시)

※ 통신모듈 : DVT 외 필드 테스트, HW 시험 (RF 검증, 신뢰성 검증) 등 제휴단말 대비 검증항목 많음

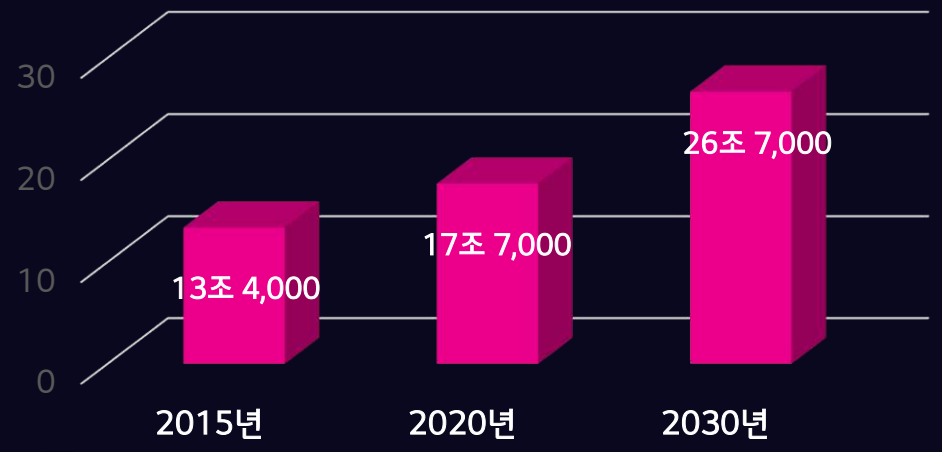
M2M 디바이스 보안사고 사례

- IoT 기기의 급속한 확산에 따라 사회안전시설, 의료장치, 가전, 자동차 및 생활용품 전반에 걸쳐 해킹 사례가 확인되고 있음
- 또한, 인터넷에 연결된 취약한 IoT 기기는 전용 검색도구로 쉽게 찾아 내어 악의적인 사용이 가능함

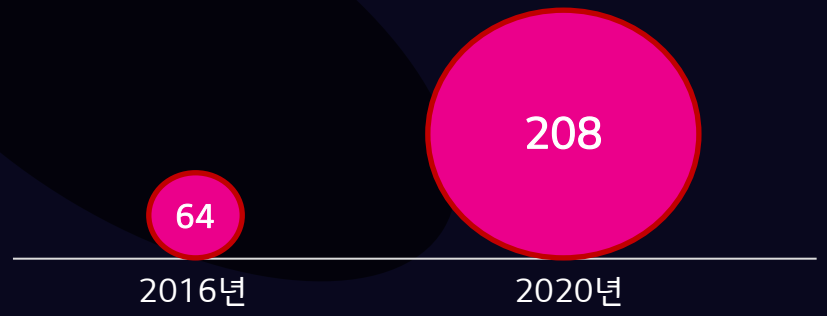


M2M 디바이스 보안사고 사례

IoT/M2M 보안사고 국내 피해 추산치 (단위: 억원)



IoT/M2M 연결 기기 급증 (단위: 억개)



IoT/M2M 보안 위협 사례

정보통신망 침입 **데이터 침해**	보안수준 낮은 기기를 노려 동신망 침입 ✓ 가정 내 **카메라, 마이크** 답재 기기 해킹 등 범죄 악용 (홈CCTV, 월패드, 로봇청소기 내 카메라 등)
디도스 공격 **악성코드 유포**	공유기 등 IoT기기 해킹 및 악성코드 업도드 ✓ 대규모 피해 단말 확보 후 DDOS 공격 환용 ✓ 또 다든 악성코드 유포 소스도 환용
살상행위	병원 내 IoT 인슐딘 펌프 조작 차댱 네트워크 침투 및 **제동/조향장치** 조작
기간시설 위협	스마트 전력망, 공항, 고속도도 등 **기간시설** 공격

관련 법령 (정보통신망 이용촉진 및 정보보호 등에 관한 법률 – 제6장 정보통신망의 안정성 확보)

제45조(정보통신망의 안정성 확보 등)

① 다음 각 호의 어느 하나에 해당하는 자는 정보통신서비스의 제공에 사용되는 **정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치**를 하여야 한다.

1. 정보통신서비스 제공자
2. 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 대통령령으로 정하는 기기·설비·장비(이하 "정보통신망연결기기등"이라 한다)를 제조하거나 수입하는 자

② 과학기술정보통신부장관은 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침(이하 "정보보호지침"이라 한다)을 정하여 고시하고 제1항 각 호의 어느 하나에 해당하는 자에게 이를 지키도록 권고할 수 있다.

③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다.

1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치
2. 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치
5. 정보통신망연결기기등의 정보보호를 위한 기술적 보호조치

④ 과학기술정보통신부장관은 관계 중앙행정기관의 장에게 소관 분야의 정보통신망연결기기등과 관련된 시험·검사·인증 등의 기준에 정보보호지침의 내용을 반영할 것을 요청할 수 있다.

제45조의2(정보보호 사전점검)

① 정보통신서비스 제공자는 새로이 **정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획 또는 설계에 정보보호에 관한 사항을 고려**하여야 한다.

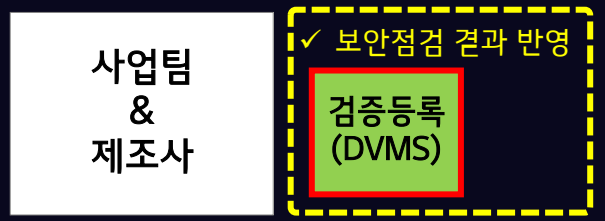
② 과학기술정보통신부장관은 다음 각 호의 어느 하나에 해당하는 정보통신서비스 또는 전기통신사업을 시행하고자 하는 자에게 대통령령으로 정하는 정보보호 사전점검기준에 따라 보호조치를 하도록 권고할 수 있다.

1. 이 법 또는 다른 법령에 따라 과학기술정보통신부장관의 인가·허가를 받거나 등록·신고를 하도록 되어 있는 사업으로서 대통령령으로 정하는 정보통신서비스 또는 전기통신사업
2. 과학기술정보통신부장관이 사업비의 전부 또는 일부를 지원하는 사업으로서 대통령령으로 정하는 정보통신서비스 또는 전기통신사업

③ 제2항에 따른 정보보호 사전점검의 기준·방법·절차·수수료 등 필요한 사항은 대통령령으로 정한다.

U+ 개발보안 프로세스

품질검증 프로세스



보안점검 항목 및 자가진단 방법



인 증

사용자 인증

인증정보의 안전한 사용

기기 인증



암 호

안전한 암호 알고리즘 사용



데이터 보호

전송 데이터 보호

저장 데이터 보호

안전한 세션 관리



플랫폼 보호

소프트웨어 보안

안전한 업데이트

보안 관리

감사 기독



물리적 보호

묻리적 인터페이스 보호

분류	인증 – 사용자 인증	위험도	Low

취약점 명

AU 1-1 처음 기기를 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.

취약점 설명

	Router Brand	Default IP Address	Default Username	Default Password
1	3Com	http://192.168.1.1	admin	Admin
2	Belkin	http://192.168.2.1	admin	admin
3	BenQ	http://192.168.1.1	admin	Admin
4	D-Link	http://192.168.0.1	admin	Admin
5	Digicom	http://192.168.1.254	admin	Michelangelo
6	Linksys	http://192.168.1.1	admin	Admin
7	Netgear	http://192.168.0.1	admin	password
8	Sitecom	http://192.168.0.1	sitecom	Admin
9	Asus	http://192.168.1.1	admin	admin
10	Synology	http://192.168.1.1	admin	Admin
11	Arris	http://192.168.0.1	admin	password

라우터 제조사별 디폴트 계정 리스트

초기 패스워드를 변경하지 않고 사용하는 경우 위 그림과 같이 공개된 디폴트 계정을 통해 인가되지 않은 사용자가 접근할 수 있다.

점검 사항 (Self-Check)

1. 디바이스에 직접 접속하여 기능을 사용하거나 설정할 수 있는가 ? (예. 공유기(AP) 관리자 페이지)
   1-1. 접속 방법 및 사용가능 기능 내역은 ?
   1-2. ID/패스워드 로그인을 사용하는 경우
      ① 최초 패스워드 생성 규칙은? 기기별로 고유한가 ? 어떻게 사용자에게 전달되는가?
      ② 최초 패스워드로 로그인 성공 시 패스워드를 변경하도록 하고 있으며 이 때 허용하는 패스워드 조합은?
2. 초기 패스워드가 기기별로 고유하며 디바이스 또는 포장박스의 특정 위치에 부착되어 전달되는가?

적격 기준

- 새로운 디바이스를 시동하여 사용자 인증이 필요한 기능에 접근을 시도한 후 인증정보를 설정하도록 요구하거나 초기 인증정보를 입력하도록 요구
- 초기 인증정보의 입력을 요구하는 경우 초기 인증 후에 이를 변경하도록 요구
- 초기 패스워드가 안전하게 전달되고 기기별로 고유하면 취약하지 않음
- 인증정보 설정 혹은 초기 인증번호를 변경하지 않고 우회하여 사용자 인증이 필요한 기능에 접근 가능하지 않음

분류	인증 – 사용자 인증	위험도	High
취약점 명	AU 1-2 관리서비스 및 중요정보 접근 시 사용자 신원을 검증하기 위해 식별 및 인증이 선행되어야 한다.		

취약점 설명



중요정보

인증정보, 센싱정보, 제어명령, 보안정책, 암호키, 개인영상정보, 개인정보 등을 말하며,
제품의 특성에 따라 다른 정보(CCTV 영상 등)들도 중요정보가 될 수 있음

관리기능

동작을 결정할 수 있는 관리기능(규칙 추가/변경/삭제/조회 등)
기능에 대한 관리기능(활성화/비활성화/시작)
기기의 설정에 대한 관리기능(설정변경/조회)
사용자 계정, 권한에 대한 관리 기능(계정 추가/변경/삭제/권한부여 등)

점검 사항 (Self-Check)

1) 디바이스에 대한 관리/설정 기능이 제공하고 있을 경우 접근 권한을 검증하는가?
2) 민감한 정보를 제공하고 있을 경우 접근 권한을 검증하는가?
3) 관리자 권한과 일반 사용자 권한이 분리되어 있는가?

적격 기준

<관리기능 및 중요정보 접근 시>
- 디바이스의 관리서비스 및 중요정보에 접근을 시도 시에 인증을 요구
- 계정에 부여된 권한을 통해 관리자와 일반 사용자를 구분하는 경우,
  . 관리자 계정으로 관리기능 및 중요정보 접근
  . 일반 사용자 계정으로는 관리서비스 접근 거부

분류	인증 – 사용자 인증	위험도	Low
취약점 명	AU 1-3 잘못된 인증정보를 통한 반복된 인증 시도를 제한해야 한다.		

취약점 설명



잘못된 인증정보 입력을 통한 반복된 인증시도를 허용하는 경우 무차별 대입공격(Brute Force Attack)을 통해 IoT기기로 비인가 접근을 허용
정확하지 않은 인증정보를 이용하여 반복적인 로그인을 시도하지 못하도록 적절하게 대응하는 기능이 필요

점검 사항 (Self-Check)

1) 패스워드 무차별 대입 공격에 대한 대책이 적용되었는가? (캡챠, 실패 시 패스워드 입력시간 간격 지연 로직 적용, 패스워드 오입력 횟수 제한 등)

적격 기준

- 잘못된 인증정보를 통한 반복된 인증 시도 시 이를 제한하고 있는 내용이 포함되어 있으며 기재된 방법이 요구사항을 대응하기에 적절 여부
- 제출문서에 기재된 대로 대응 방법 실제 구현 여부

분류	인증 – 인증정보의 안전한 사용	위험도	High
취약점 명	AU 2-1 인증정보는 하드코딩 되거나 평문으로 저장되지 않아야 한다.		

취약점 설명

안전하지 않은 코드의 예 JAVA

```
public class MemberDAO {
    private static final String DRIVER = "oracle.jdbc.driver.OracleDriver";
    private static final String URL  = "jdbc:oracle:thin:@192.168.0.3:1521:ORCL";
    private static final String USER = "SCOTT"; // DB ID;
//DB 패스워드가 소스코드에 평문으로 저장되어 있다.
    private static final String PASS = "SCOTT"; // DB PW;
.....
    public Connection getConn() {
        Connection con = null;
        try {
            Class.forName(DRIVER);
            con = DriverManager.getConnection(URL, USER, PASS);
 ......
```

획득한 중요정보(인증값, 암호키)는 2차 공격의 중요한 정보를 제공함

점검 사항 (Self-Check)

1) 소스코드 또는 설정파일에 하드코딩 되어 있는 패스워드, 암호키 등 정보가 존재하는가?
2) 백업 등의 기능을 이용하여 파일 형태로 Export 하는 기능이 존재하는가?
   존재한다면, Export 시 중요 정보에 해당하는 파일의 존재여부 및 해당 파일의 평문화 Export 여부는?

적격 기준

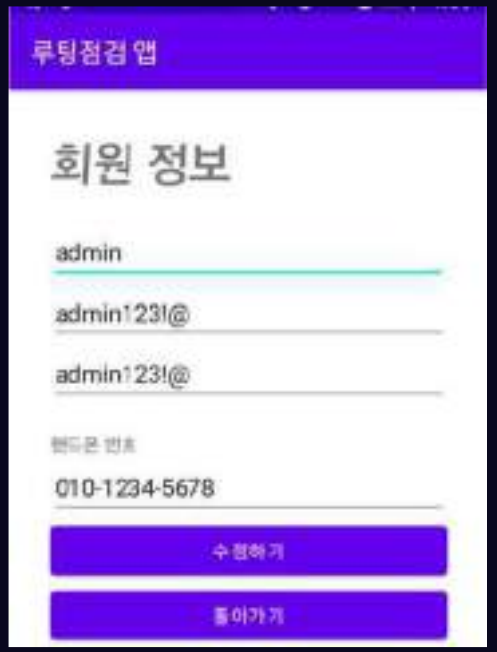
- 디바이스 내에 저장된 인증정보가 안전한 방식으로 암호화되어 있으며 암호키도 안전하게 보관됨
- 사용자 계정 및 중요 설정정보를 파일 형태로 추출(Export)하는 기능이 있는 경우 추출된 파일이 암호화되어 있음
- 메모리에 평문으로 로드되어 사용된 중요정보(암호키, 인증정보)는 사용 후 즉시 삭제하고 있음

분류	인증 – 인증정보의 안전한 사용	위험도	Low

취약점 명

AU 2-2 인증을 위한 비밀번호 입력 시 화면에 노출되지 않도록 마스킹 처리해야 한다.

취약점 설명



잘못된 사례



안전한 적용 사례

점검 사항 (Self-Check)

1) APP 및 웹페이지 등의 서비스상의 인증 요구 화면에서 비밀번호 입력 시 '*'등으로 마스킹 처리되어 있는가?
2) 비밀번호 변경 기능상에서 비밀번호 입력 시 '*' 등으로 마스킹 처리되어 있는가?

적격 기준

디바이스에서 제공하고 있는 모든 인증 기능에 대해 아이디/비밀번호 메커니즘을 사용하는 경우 비밀번호가 화면에 마스킹 되어 있음

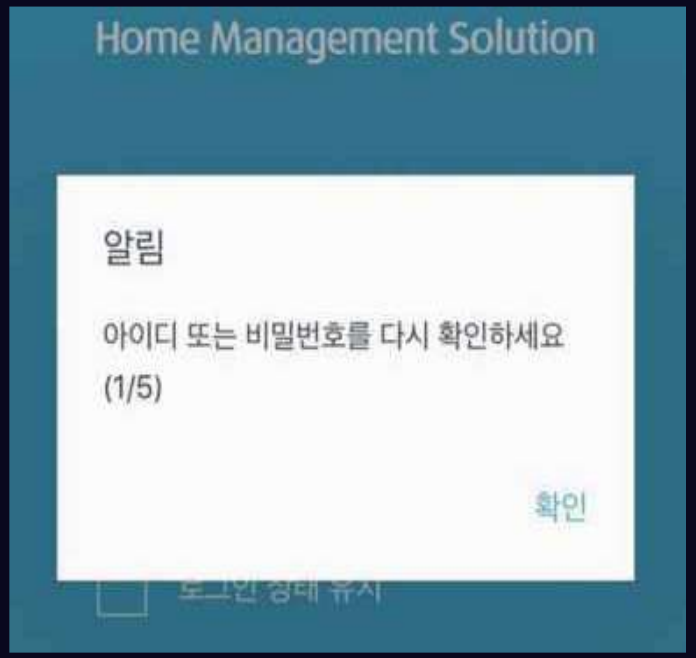
(입력 당시 평문으로 보이다가 곧 마스킹 처리되는 경우는 양호한 것임)

분류	인증 – 인증정보의 안전한 사용	위험도	Low

취약점 명

AU 2-3 인증 실패 시 실패 사유에 대한 피드백 정보를 제공하지 않아야 한다.

취약점 설명



인증 실패 사유에 대한 구체적인 피드백은 인증시도 공격의 정보를 제공
- 존재하지 않는 아이디입니다. 또는 아이디가 일치하지 않습니다.
- 패스워드가 잘못 되었습니다.

- 사용자 로그인 실패 사유를 구체적으로 유추할 수 없도록 단순하고 동일한 피드백 정보 (로그인 실패 등)만 출력되도록 해야 한다.

점검 사항 (Self-Check)

1) 인증 실패(오류)시 그 실패(오류) 사유를 아래 중 어떻게 안내 하는가?
① 존재하지 않는 아이디 입니다. (또는, 패스워드가 일치하지 않습니다.) → 각각 해당 상황에 맞게 자세히 안내 여부
② 아이디 또는 패스워드가 일치하지 않습니다. → 아이디가 틀렸는지 패스워드가 틀렸는지 모르도록 애매하게 안내 여부

적격 기준

- 잘못된 인증정보 입력으로 인증실패 후 생성되는 알림 메시지가 인증 실패 사유 혹은 피드백을 제공하고 있지 않거나 후속 공격을 하지 못하는 범위에서 사유 제공 (예. 아이디 또는 패스워드가 일치하지 않습니다.)

분류	인증 - 기기인증	위험도	High

취약점 명

AU 3-1 기기는 각각의 고유 식별정보를 보유해야 한다.

취약점 설명



디바이스 식별자가 고유하지 않을 경우
악의적인 디바이스에 의한 서비스 부정 사용, 거짓 정보 수신,
상용 디바이스 서비스 플랫폼에 대한 악의적인 공격 발생 시,
해당 디바이스를 식별할 수 없는 문제가 발생

점검 사항 (Self-Check)

1) 디바이스 식별하기 위해 사용하는 고유 식별 정보는?
   예. 모델명, 제조사, 시리얼넘버, MAC address, home ID(z-wave), IMEI, CTN, PSK(Pre-Shared Key)
2) PSK(Pre-Shared Key)를 사용하는 경우 디바이스별 고유 여부 와 생성 규칙은?
3) “기기 식별정보(하드웨어 모델 정보, 소프트웨어·펌웨어 버전 정보)”를 사용자에게 제공하고 있는가? 어떤 수단으로 해당 정보를 사용자에게 제공하고 있는가?

적격 기준

- 디바이스 제조사의 고유 식별번호 정책을 확인하고 해당 정책에 따라 식별번호 부여 여부
- “기기 식별정보(하드웨어 모델 정보, 소프트웨어·펌웨어 버전 정보)”를 사용자에게 제공

분류	암호 – 안전한 암호 알고리즘 사용	위험도	Low

취약점 명

CR 1-1 암호화시 안전한 암호 알고리즘을 사용해야 한다.

취약점 설명



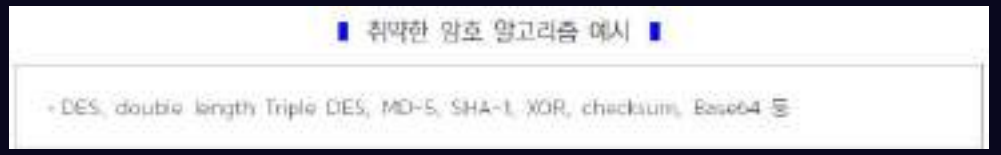
구분		암호 알고리즘
대칭키 암호 알고리즘		- SEED, HIGHT - ARIA-128/192/256 - LEA-128/192/256 - AES-128/192/256 - 3TDEA
해시 함수	단순해시(전자서명용)	- SHA-1 / HAS-160 * 112비트/128비트 보안강도를 제공하지 못하므로, 메시지 인증/구성도/난수생성용으로만 사용 가능함
	메시지인증/구성도/난수생성용	- SHA-224/256/384/512 - SHA-512/224, SHA-512/256 - SHA3-224/256/384/512 - LSH-224/256/384/512 - LSH-512/224, LSH-512/256
공개키 암호 알고리즘	키 공유용	- [인수분해 문제] DH, MQV - [타원곡선] ECMQV, ECDH
	암·복호화용	- [인수분해 문제] RSAES, RSA
	전자서명용	- [인수분해 문제] RSA-PSS, RSA - [이산대수 문제] KCDSA, DSA - [타원곡선] ECDSA, EC-KCDSA, ECDSA



보안강도에 따른 공개키 암호 알고리즘 분류

보안강도	인수분해 문제(비트)	이산대수 문제(비트)		타원곡선(비트)
		공개키	개인키	
112 비트	2048	2048	224	224
128 비트	3072	3072	256	256
192 비트	7680	7680	384	384
256 비트	15360	15360	512	512

취약하거나 안전성이 검증되지 않은 암호 알고리즘(보안강도 112비트 미만)은 사용되지 않도록 제거하거나 비활성화 해야한다.



취약한 암호 알고리즘 예시

- DES, double length Triple DES, MD-5, SHA-1, XOR, checksum, Base64 등

TDES(보안강도 112비트)는 기존 암호화된 데이터를 복호화하는 용도로만 사용을 권고한다.

점검 사항 (Self-Check)

1) 암호화 적용 시 대상별 사용하고 있는 알고리즘은?
   예. ① 대칭키 암호화 AES128 이상, ② 비대칭키인 경우 RSA(2,048 비트 이상), ECDSA(256 비트 이상)
2) 일방향 암호화인 경우 SHA(256 비트 이상 + salt 사용)

적격 기준

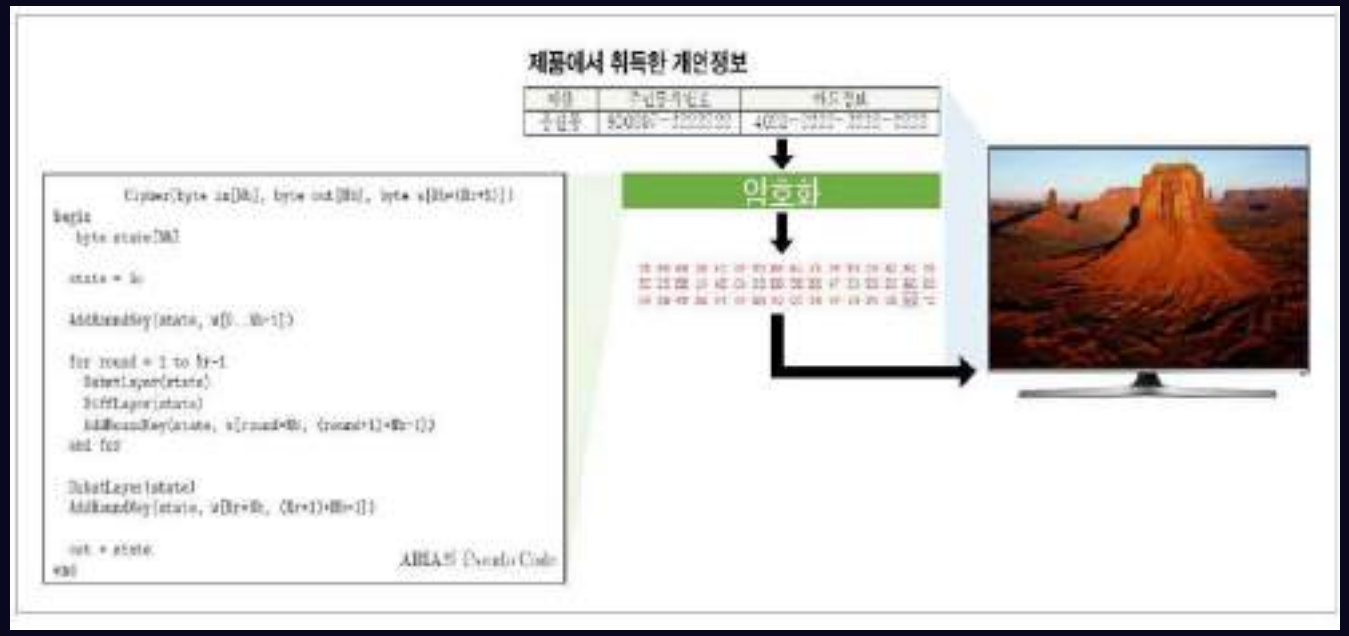
- 대칭키 암호화 AES128 이상, 비대칭키는 2,048 비트 이상 사용, 일방향 암호화는 SHA 256 비트 이상 + salt 사용
- 취약한 암호 알고리즘이 disable 되어 있어야 함

분류	데이터 보호 – 전송 데이터 보호	위험도	High

취약점 명

DP 1-1 기기 간 전송되는 중요정보는 암호화하여 전송해야 한다.

취약점 설명



중요정보 전송시에는 암호화 전송 또는 암호화 통신해야 함

점검 사항 (Self-Check)

1) 디바이스에서 서버(플랫폼)로 전송되는 중요정보에는 어떤 것들이 있는가? (중요정보의 예 : 인증정보, 암호키, 개인영상정보, 결제정보)
   ① 암호화하여 전송하는 경우 사용된 암호화 알고리즘은 무엇인가? (비표준 암호화 알고리즘인 경우 세부 내역 및 인증 획득 관련 사항 기술)
2) 디바이스 개통 시 AllJoyn을 통한 Soft AP를 사용하는 경우 암호화 통신을 하는가? 이 때 암호키는 어떻게 생성하여 앱과 디바이스간 교환하는가?

적격 기준

- 전송되는 중요정보 목록을 확인
- 중요정보를 암호화한 알고리즘은 적합한가? (CR 1-1 항목에 따름)
- 전송 방법은 무엇인가?

분류	데이터 보호 – 전송 데이터 보호	위험도	Low

취약점 명

DP 1-2 알려진 프로토콜 기반으로 통신 채널 생성 시 안전한 보안 모드를 사용해야 한다.

취약점 설명



점검 사항 (Self-Check)

1) TLS 사용 시 TLS ver1.2 이상만을 사용하는가?
2) ZigBee, Bluetooth, Z-wave, CoAP, MQTT, WiFi 등 신뢰된 암호통신 프로토콜 사용 및 암호알고리즘을 사용하는가?

적격 기준

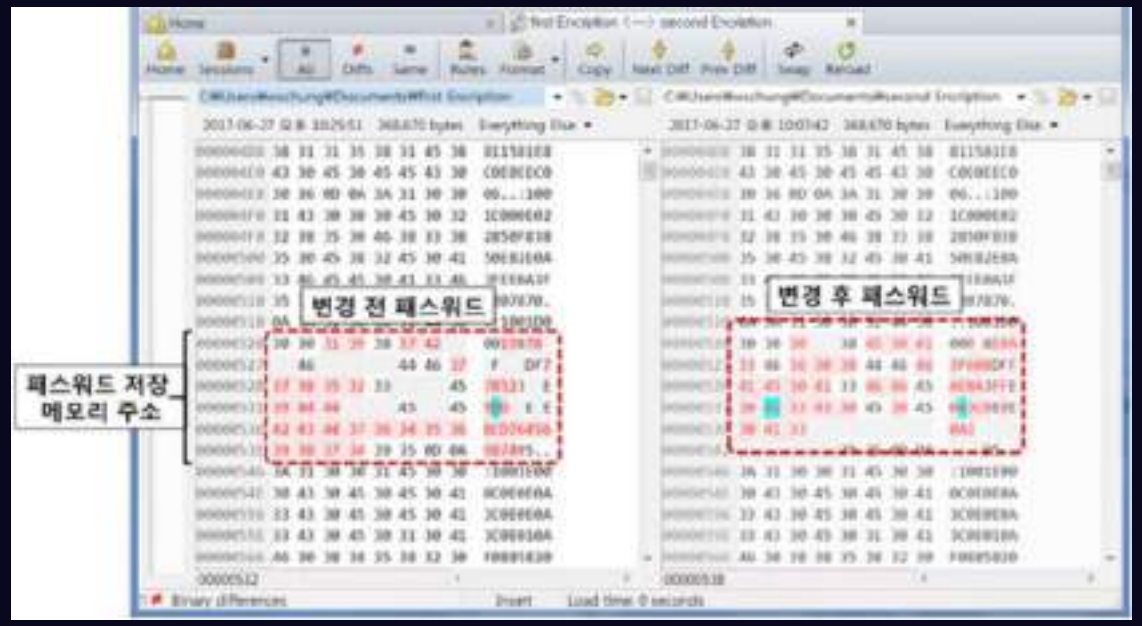
- 프로토콜 설계의 결함이 있는 SSLv2, SSLv3, TLSv1.0은 비활성화 필수 (신규 서비스의 경우) TLSv1.3 이상 사용
- 블루투스에서는 암호화된 인증 페어링 또는 암호화된 저전력 보안연결 인증 적용
- WiFi : WPA2 방식 적용
- 비표준 암호화 방식 사용시 재생공격(replay attack) 방지 대책 적용

분류	데이터 보호 – 저장 데이터 보호	위험도	High

취약점 명

DP 2-1 기기에 저장되는 중요정보는 암호화해야 한다.

취약점 설명



암호화 적용 대상 중요정보

- 인증정보(비밀번호, 지문정보, 홍채정보, 정맥정보 등)
- 개인정보(이름, 주소, 생년월일, 신용카드번호, 위치, 건강정보 등)
- 데이터 암호화 키, 기기 운영을 위한 설정값(IP/MAC 정보 등)

중요 정보는 암호화하여 저장하거나 중요 정보에 대하여 접근통제를 적용한다.

점검 사항 (Self-Check)

- 디바이스 내 개인정보/민감정보/계정정보 등 인증정보 등을 저장하고 있는가?

1) 해당 정보 내역과 어떤 경로에 저장되는가?
2) 개인정보 및 인증정보가 추출 가능한 저장 매체(USB, SD카드 등)에 저장되는가? 원격에서 접근 가능한가?
3) 암호화하여 저장하고 있는 경우, 적용된 암호화 표준은?
4) 휘발성 메모리에 로드되는 중요정보(암호키, 인증정보 등)는 사용 후 삭제하고 있는가?

적격 기준

- 저장되는 중요정보 별로 암호화 저장방식이 적절한가? (CR 1-1)
- 메모리상에 로드되는 중요정보(암호키, 인증정보 등)는 사용 후 삭제하고 있는가?

분류	데이터 보호 – 안전한 세션 관리	위험도	Low
취약점 명	DP 4-1 세션 연결 후 일정시간 동안 미사용 시 세션을 잠그거나 종료시켜야 한다.		

취약점 설명



사용자 또는 다른 기기에 연결된 세션이 오랫동안 사용되지 않을 경우
제3자에 의해 악용되어 중요정보 유출의 발생 및 세션 정보를 도용하여 기기에 접근할 수 있다.

점검 사항 (Self-Check)

1) 일정 시간동안 동작이 없는 경우 디바이스는 사용중인 세션을 종료하거나 사용을 중지하여야 하는데, 세션 및 토큰 값의 파기 주기는 어떻게 되는가?
2) 세션 종료(잠금) 후 재접속시 재인증을 수행하는가?

적격 기준

- 세션 잠금 또는 세션 종료 시간(기기 특성에 적합 여부)은 어떻게 설정되어 있는가?
  예. 민감한 제어 명령 처리가 포함되는 세션은 30초 이후 세션을 잠금 또는 종료, 민감하지 않은 제어 명령 처리 세션은10분 이후 잠금 또는 종료
  (참고로, LG유플러스 세션 타임아웃 정책은 환경에 따라 30분~2시간, 30분 정도를 권고)
- 세션 잠금 종료 후 재접속 시 재인증을 수행하는가?

분류	플랫폼 보호 – 소프트웨어 보안	위험도	Low

취약점 명

PL 1-1 보안약점이 존재하지 않도록 시큐어코딩을 적용해야 한다.

취약점 설명





시큐어 코딩이 적용되지 않은 경우 입력 데이터 검증, 보안기능, 에러처리, API 오용 등에서 보안 취약점이 발생 할 수 있음
보안 취약점을 이용한 사용자 정보 수집(공유기, IP카메라, IoT앱 등에서 사용자 정보 수집하기 위한 공격이 이루어짐

점검 사항 (Self-Check)

1) 구현한 코드 내에 취약한 API(strcpy, strcat, sprintf, strtok, strlen, gets, 길이 제한없이 fscanf/sscanf 사용, 포맷 정의없이 printf 사용 등) 사용 여부는?
2) 해당 취약 API 인자 값으로 외부로부터의 입력값(사용자 입력/외부 포트로부터의 입력/별도 외부 파일의 내용 로딩 후 사용 등)을 검증없이 호출 여부는?
3) 소프트웨어 개발보안 가이드를 참고하여 시큐어 코딩을 적용하였는가 ?
   - 소프트웨어 개발보안 가이드(행정안전부/한국인터넷진흥원, 2019), JAVA 시큐어 코딩 가이드(행정자치부, 2012), C 시큐어 코딩 가이드(행정자치부, 2012)
   - Andriod-JAVA 시큐어 코딩 가이드(안전행정부, 2011), ISO/IEC TS 17961:2013(C secure coding rules)
4) Codesonar, Sparrow, Fortify 등의 소스취약점 점검 툴을 이용하였는가?

적격 기준

- 소스 취약점 점검 결과 보고서 상에 중요 취약점을 보유하고 있는가?
- 펌웨어 리버싱 시에 취약한 함수 사용 또는 입력값 필터링 없이 시스템 명령을 실행하고 있는가?
- fuzzing 공격 대책 적용 여부 진단 방법 강구 필요

분류	플랫폼 보호 – 소프트웨어 보안	위험도	Low

취약점 명

PL 1-2 알려진 보안취약점 존재여부를 확인하고 제거하여야 한다.

취약점 설명

▮ 알려진 보안취약점 예시(스마트 락 모바일 앱) ▮

(CVE-2019-13143)



☞ 공개영역 보안취약점 DB(CVE)에 보고된 스마트 락(FB50)의 파라미터 변조 취약점

(펌웨어 파일 추출)



☞ 스마트 락(FB50)의 파라미터 변조 취약점을 이용하여 공격자가 FB50의 소유권 획득에 성공한 공격

▮ 공개영역 보안취약점 정보 예시 ▮

보안취약점 공개영역	내용
https://owasp.org	웹, IoT 기기, Mobile App 관련 취약점 공개
http://www.cve.mitre.org	미국 NIST 공개 취약성 DB
http://cwe.mitre.org	미국 NIST 공개 취약성 DB
http://www.securityfocus.com	취약점 공개 사이트
http://www.exploit-db.com	취약점 공개 사이트
http://secunia.com	취약점 공개 사이트
http://www.packetstorm.com	취약점 공개 사이트
http://www.krcert.or.kr	CERT 사이트(KISA)
http://www.kiisc.or.kr	한국정보보호학회 학회지, 논문지
https://csenic.or.kr	국가지정 컴퓨터 연구정보센터 논문지
3자 제공 소프트웨어 정보(예시)	OpenSSL,OpenSSH 등

공개된 취약점에 대해서는 공격코드도 공유되기 때문에
주기적으로 공개영역 조사를 통해 해당되는 보안취약점이 존재하는지
확인하여 제거해야 한다.

점검 사항 (Self-Check)

펌웨어 개발 시 사용했던 OS, 프로토콜, 라이브러리, API, 패키지, 오픈소스의 종류는 무엇이며 각각의 버전 정보는?

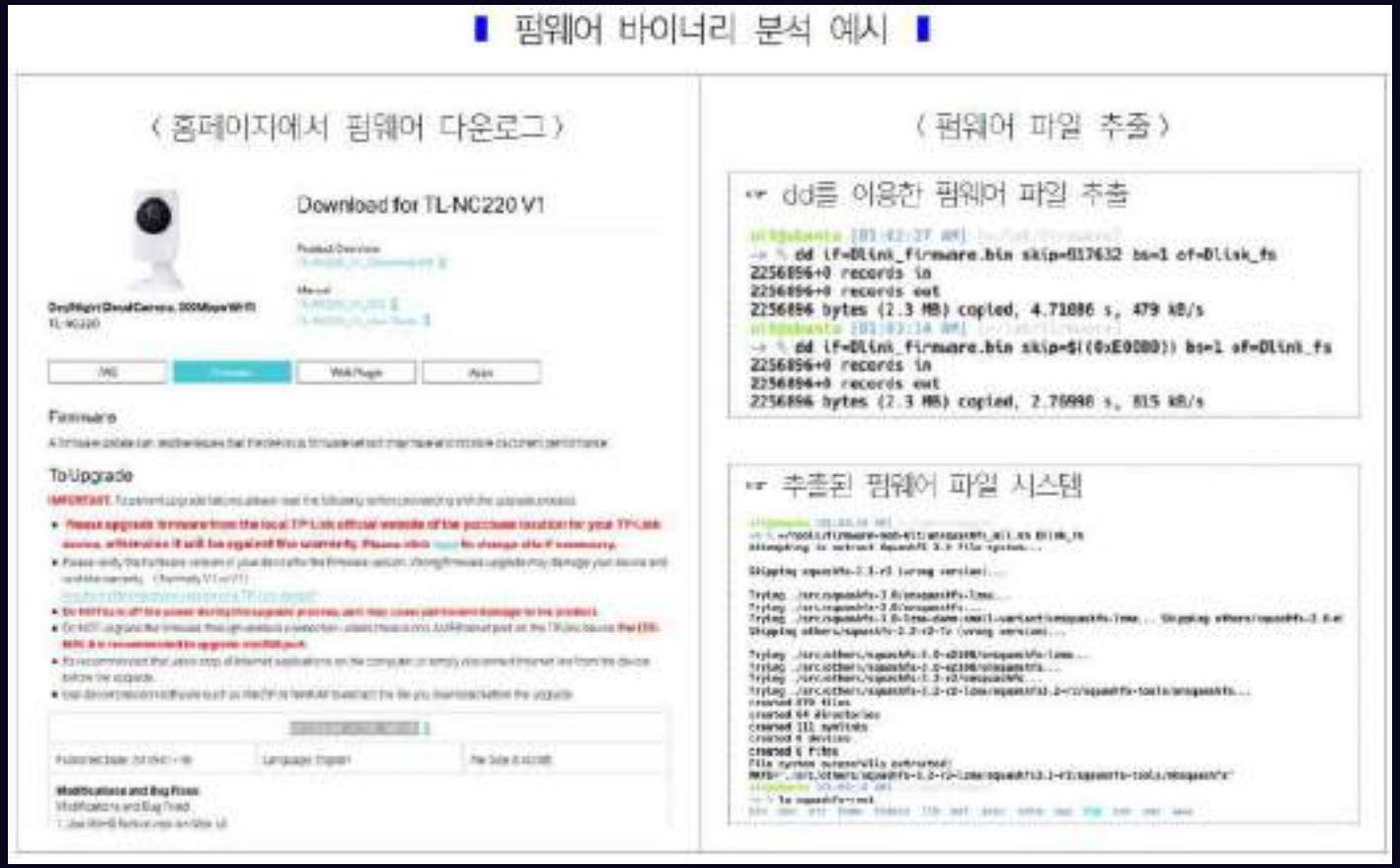
적격 기준

사용 중인 프로토콜, 라이브러리, API, 패키지, 오픈소스의 버전에 취약점이 부재함
취약한 OS 버전을 사용 중인가?

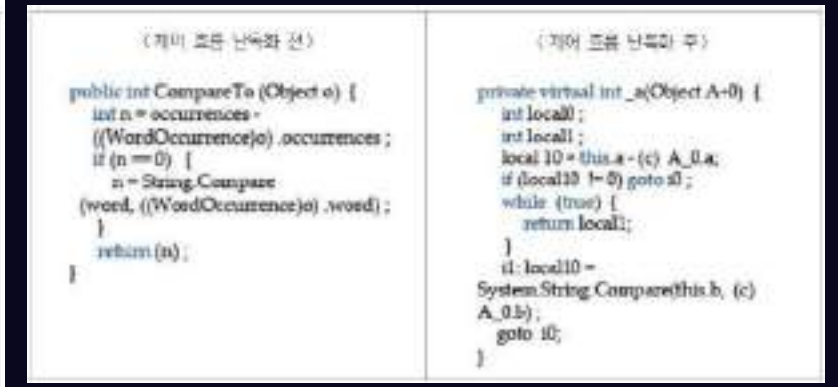
분류	플랫폼 보호 – 소프트웨어 보안
위험도	Low
취약점 명	PL 1-3 소스코드 분석 방지를 위해 난독화를 적용해야 한다.

취약점 설명

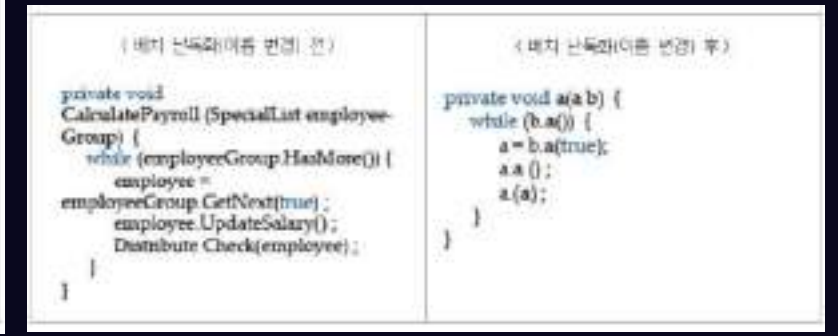
펌웨어 바이너리 분석 예시



제어 흐름 난독화 적용 예시



배치 난독화(이름 변경) 적용 예시



점검 사항 (Self-Check)	1) 펌웨어에 대한 소스코드 난독화 처리를 수행하였는가? 2) 적용한 소스코드 난독화 솔루션은 무엇인가?
적격 기준	- 펌웨어 상의 주요 실행코드에 대한 소스코드 복원(디컴파일)을 시도하여 난독화 여부를 확인

분류	플랫폼 보호 – 안전한 업데이트	위험도	High

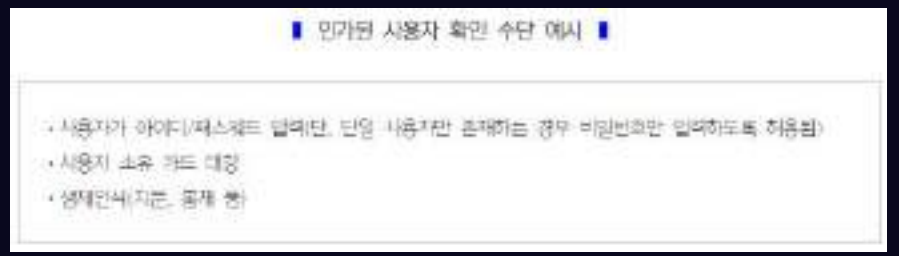
취약점 명

PL 2-1 업데이트 수행 전 인가된 사용자(및 관리자) 여부를 확인해야 한다.

취약점 설명







위장된 업데이트 서버를 통해 업데이트 파일이 배포되거나 사용자 인증절차 없이 업데이트 파일이 적용되는 경우 기기로 악성코드 등이 유입될 수 있음
신뢰할 수 있는 업데이트 서버 여부의 검증, 업데이트를 수행하는 사용자에 대한 인증 수행

점검 사항 (Self-Check)

1) 디바이스의 펌웨어 업데이트는 인가된 디바이스만 업데이트 되도록 인증을 하는가 ?
2) 수동으로 펌웨어를 업데이트하는 기능이 제공되는 경우 해당 기능을 사용하기 전에 권한 보유자만 업데이트 하도록 인증을 적용하였는가?
3) 외부 포트(예. USB, SD카드 등)를 통해 펌웨어 업데이트를 허용하고 있는가? 허용할 경우 인가된 사용자만 업데이트를 허용하는 절차는?
4) 업데이트를 수행하기 전에 업데이트 서버를 검증하는가? 업데이트 서버 인증서의 유효성 검증(OCSP/CRL 폐기 여부 확인, 유효기간 검증 등)

적격 기준

- 비인가자에 의한 펌웨어 업데이트가 불가
- 펌웨어 업데이트 시 대상 디바이스를 안전한 방법으로 인증
- 외부 포트를 이용한 펌웨어 업데이트를 허용하고 있을 경우 사용자의 인증 절차의 존재
- 단말이 업데이트 서버를 검증 여부 확인
- 자동 업데이트 기능을 제공하는가? (단, 자동 업데이트 기능은 Standard Recommend 항목으로 점검항목에서 제외함)

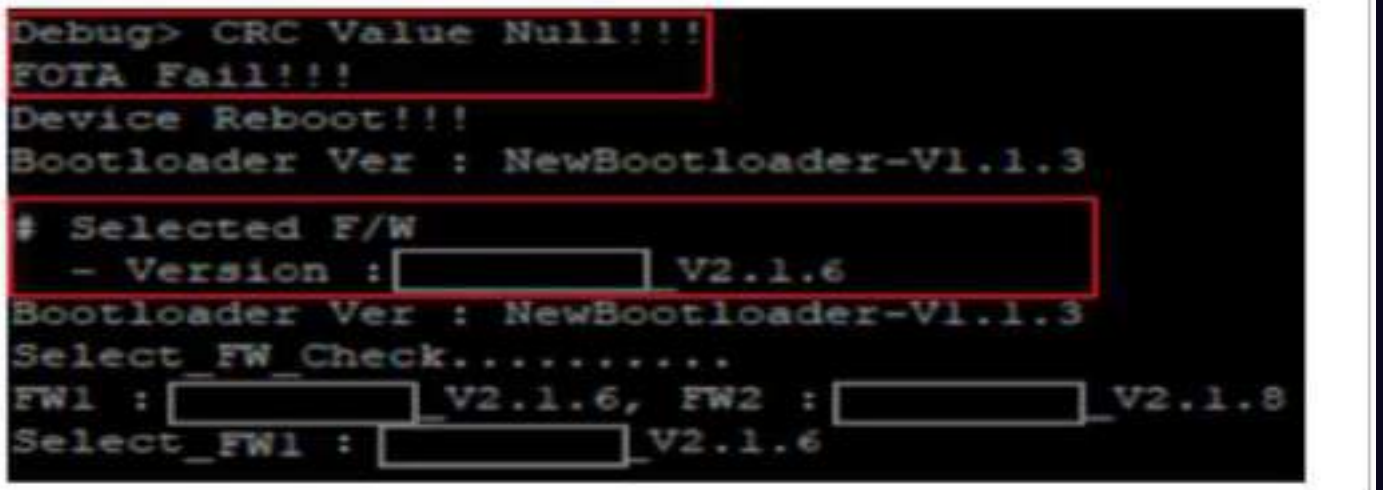
분류	플랫폼 보호 – 안전한 업데이트	위험도	Low

취약점 명

PL 2-2 업데이트 실패 시 롤백 기능을 지원해야 한다.

취약점 설명

☞ 대기질 측정 센서에서의 FOTA를 이용하여 펌웨어 업데이트 실패(버전 : 2.1.8) 시 롤백 기능이 적용되어 기존 펌웨어 버전(2.1.6)으로 자동 복구된다.



자동/수동 업데이트 설치 실패 시 안전한 기존 버전으로 복구하는 수단을 제공해야 하며
복구된 기기는 오류, 서비스 거부 또는 데이터 손실 없이 정상적인 운영상태를 유지해야 한다.

점검 사항 (Self-Check)

1) 펌웨어 업데이트 실패 시 바이너리 롤백 프로세스가 있는가?
2) 펌웨어 롤백 절차는?

적격 기준

- 기능 시험을 통해 업데이트 실패 시 롤백 기능 확인
- 기능 시험을 통해 롤백 후 기기가 정상 동작하는지 확인

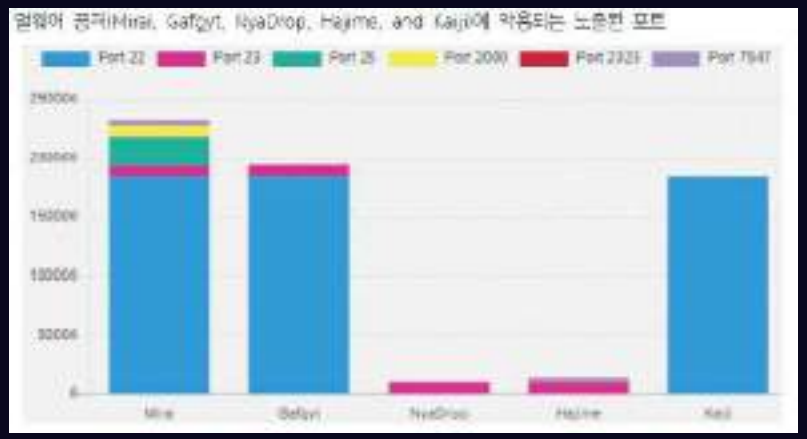
분류	플랫폼 보호 – 보안 관리	위험도	High

취약점 명

PL 3-1 불필요한 서비스(명령어)는 제거하거나 비활성화해야 한다.

취약점 설명

TCP 포트	서비스	열린 포트(수)	노출 포트 비율
443	HTTPS	772,258	35.6%
80	HTTP	670,789	30.9%
22	SSH	184,848	8.5%
3389	RDP	40,893	1.9%
8443	HTTPS_Alt	39,100	1.8%
8080	HTTP_Alt	30,502	1.4%
21	FTP	30,059	1.4%
8001	HTTP_Alt	27,187	1.3%
25	SMTP	23,901	1.1%
8000	Applications	21,028	1.0%



기기 운영에 불필요한 네트워크 서비스(포트, 명령어 등) 존재 시 공격자는 해당 네트워크 서비스의 보안 취약점을 악용하여 기기의 무력화 또는 우회 시도할 수 있음

점검 사항 (Self-Check)

1) 디바이스에서 제공하여야 하는 필요 서비스는 무엇인가?
2) Telnet, FTP, UPnP, SNMP가 활성화되어 있는가?
3) 외부 접속이 허용된 경우 접근 IP 제한, 접근 비밀번호 설정 등의 추가적인 보안 조치가 되어 있는가?
4) 펌웨어 상의 불필요한 명령어들은 모두 삭제하였는가?
5) 디버깅, 시험용 코드 또는 기기 운용에 불필요한 백도어 코드 및 기능이 존재하는가? 존재 시 해당 기능의 접근 방법은?
6) 사용되지 않는 불필요한 네트워크 인터페이스(Bluetooth, WiFi, NFC, ZigBee, Z-Wave, LoRa, NB-IoT, LTE-M, 5G, RFID 등)가 활성화 되어 있는가?

적격 기준

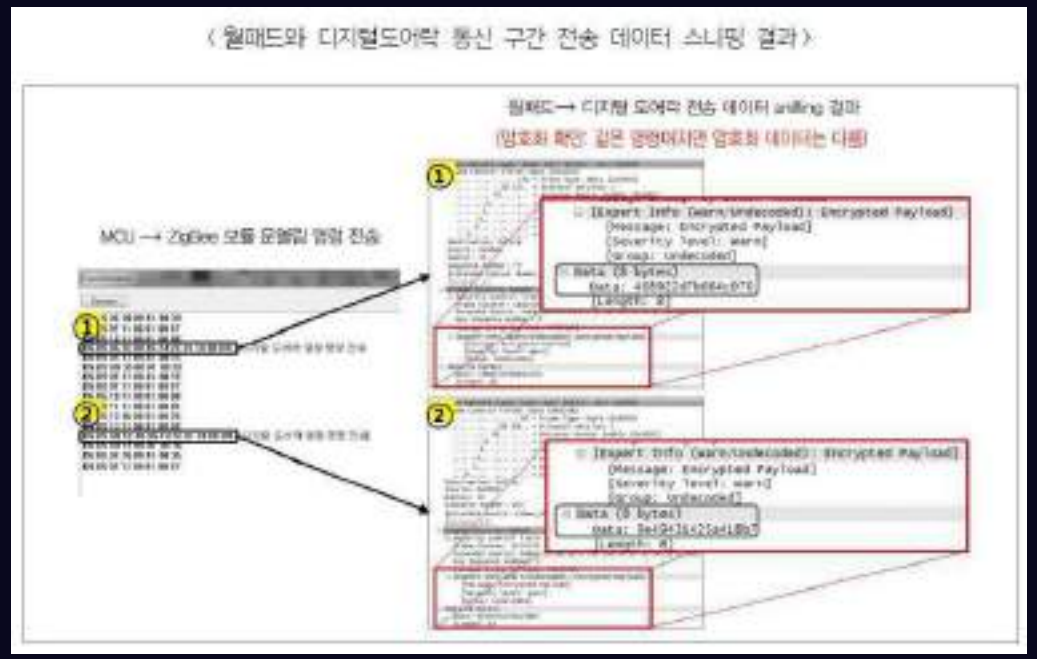
- IPv4 및 IPv6 인터페이스를 통해 불필요한 서비스가 활성화되어 있지 않음
- Telnet, FTP, UPnP, SNMP가 활성화되어 있지 않음
- 외부 접속이 허용된 경우 접근 IP 제한, 접근 비밀번호 설정 등이 적용되어 있음
- 인가된 사용자에 의해서만 서비스 활성화 기능이 수행되어야 함
- 펌웨어 상에 불필요한 명령어들의 존재 여부 확인
- 디버깅, 시험용 코드 또는 기기 운용에 불필요한 백도어 코드 및 기능이 존재 여부 확인

분류	플랫폼 보호 – 보안 관리	위험도	High

취약점 명

PL 3-2 원격관리는 신뢰할 수 있는 환경에서 수행되어야 한다.

취약점 설명







관리/제어를 위한 접속 시 인증 절차가 없거나 데이터가 보호되지 않으면 비인가 접근을 허용할 수 있으며 기기의 제어권이 탈취될 수 있음

점검 사항 (Self-Check)

- 디바이스 내 원격 접근 서비스가 존재하는가?
  1) 존재한다면 접근 제어 설정이 되어 있는가?
  2) 계정 사용시, 모든 디바이스에 공통된 계정을 사용하는가? 공통된 계정 사용시, 계정정보 유출에 대비하여 갱신 가능한가?
  3) 패스워드 복잡도, 로그인 절차, 패스워드 무작위 대입공격 대책 적용 여부(캡챠, 실패 시 패스워드 입력시간 간격 지연로직 적용)?
  4) 원격관리는 지정된 IP에서만 안전한 인증 절차를 통해서 접근이 가능한가?

적격 기준

- 지정된 IP에서만 접근 가능 및 안전하지 않은 채널로 접근하여 원격관리 서비스 수행 불가능
- 원격관리용 계정은 적절한 인증 절차를 통해 접근 가능
- 원격관리용 계정이 디바이스 별로 유일하게 제공되지 않는 경우 계정정보 유출에 대비하여 갱신 가능

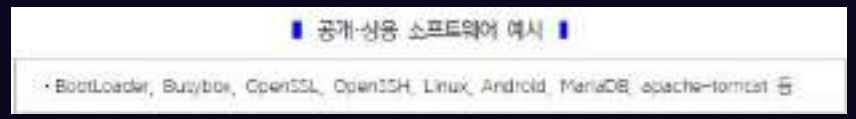
분류	플랫폼 보호 – 보안 관리	위험도	Low

취약점 명

PL 3-3 최신 보안패치가 적용된 3rd party 라이브러리를 사용해야 한다.

취약점 설명







관리/제어를 위한 접속 시 인증절차가 없거나 데이터가 보호되지 않으면 비인가 접근을 허용할 수 있으며 기기의 제어권이 탈취될 수 있음

점검 사항 (Self-Check)

- OpenSSL, OpenSSH, Bootloader, Busybox, linux 등의 오픈 소스를 사용하고 있는가?
  1) 사용한다면 설치된 오픈소스 및 버전은 어떻게 되는가?

적격 기준

- 소프트웨어 정보 홈페이지를 통해 최신 소프트웨어 버전 외 사용 여부를 확인하고 CVE에 등재되어 있지 않음

※ 확인방법 : 어플리케이션 및 Bootloader, Busybox. OpenSSL OpenSSH, Linux를 포함한 3rd Party 소프트웨어에 대한 보안 취약점 점검

분류	플랫폼 보호 – 감사 기록	위험도	Low

취약점 명

PL 4-1 보안과 관련된 이벤트는 감사기록을 생성해야 한다.

취약점 설명









사용자의 금전적 손실, 사생활 침해 등 사고에 대한 책임 추적을 위해 감사기록을 생성하고 변경/삭제가 발생하지 않도록 적절히 보호해야 함

점검 사항 (Self-Check)

1) 디바이스에서 발생하는 이벤트에 대한 감사기록을 생성하고 있는가?
※ 이벤트 대상 : 사용자 로그인 성공/실패, 제품 설정 변경 내역, 기능 수행 내역(보안기능 포함) 등
2) 감사기록 내용은 어떠한 것이 있는가?
3) 감사기록을 기기에 저장하고 있는가? 외부 서버 또는 기타 저장장치로 전송하고 있는가?

적격 기준

- 보안관련 이벤트를 수행한 후 감사기록 로그를 확인함
- 감사 기록 정보 중 비밀번호, 암호키 등의 민감정보가 존재할 경우 취약
- 감사기록은 사건발생 일시, 사건 유형, 사건을 발생시킨 주체의 신원, 작업내역 및 결과(성공/실패) 포함하여야 함

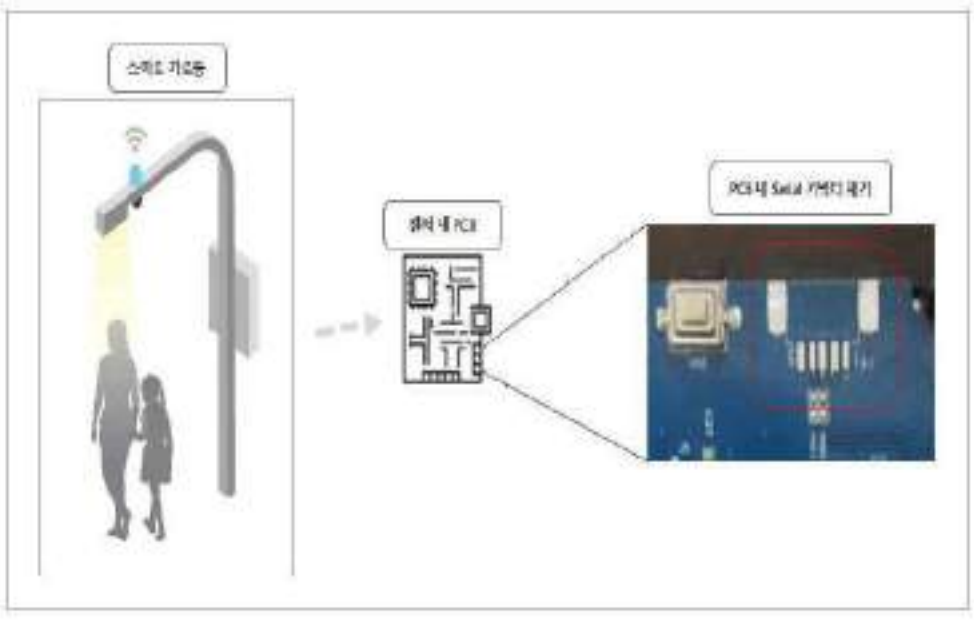
분류	물리적 보호 – 물리적 인터페이스 보호	위험도	Low

취약점 명

PH 1-1 불필요한 외부 인터페이스는 비활성화하고, 필요 시 접근통제 기능을 지원해야 한다.

취약점 설명





기기의 외부에 노출되거나 내부에 숨겨진 인터페이스에 대해 접근통제 기능이 적용되지 않은 경우
공격자는 기기 내부의 저장된 중요정보, 펌웨어 이미지 등에 접근하여 다양한 공격에 악용될 수 있음

점검 사항 (Self-Check)

- USB, Serial Port, Ethernet 포트가 디바이스 외부에 존재하는가?
  1) USB, Serial Port, Ethernet, SD카드 등의 외부 포트가 존재한다면 사용 용도 및 동작 과정은?
  2) USB, SD카드 등 외부 포트에 연결 시 자동으로 마운트 되는가?

적격 기준

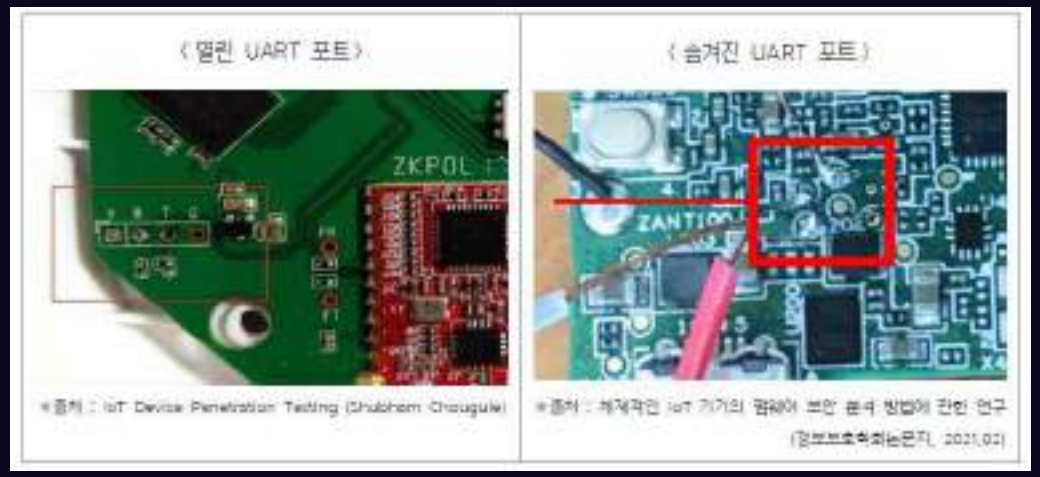
- 외부에 노출된 인터페이스의 필요 여부는 제품 사용 설명서 또는 제조사가 제공하는 문서로 확인
- USB, RS232, Ethernet 포트로 운영체제(OS) 펌웨어에 접근할 수 있을 경우 취약함
- USB, SD카드 포트의 자동 마운트가 허용되어 있고 자동 마운트 기능이 불필요시 취약함
- 필요한 외부 인터페이스라도 비인가된 접속을 방지하기 위한 접근통제 기능이 적용되었는지 확인
- 불필요한 외부 인터페이스가 존재할 경우 제거하거나 비활성화 가능 여부를 확인

분류	물리적 보호 – 물리적 인터페이스 보호	위험도	Low

취약점 명

PH 1-2 비인가자의 내부 포트 접근을 방지해야 한다.

취약점 설명





기기의 내부 인터페이스에 접근이 가능한 경우 펌웨어 추출, 명령어 Shell 획득, 동적 분석 등 다양한 공격에 악용이 가능함

점검 사항 (Self-Check)

- UART/JTAG Serial Port(또는 기타 Port)가 존재하는가?
  1) 존재할 경우 용도는 무엇인가?
  2) UART 등의 Serial Port 연결 시 로그인 절차는 ?
  3) UART/JTAG Serial Port를 통한 Shell 접근이 가능한가?
  4) Android 일 경우 adb를 통한 Shell 접근이 가능한가?
  ① 가능할 경우 용도는 무엇인가? ② 제공한다면 부여된 권한(root/일반권한)은?

적격 기준

- 제조사에서 제출한 제품 사용 설명서를 기반으로 내부 인터페이스 유무를 확인
- 특별한 사유 없이 납품시에도 UART, JTAB, ADB 접근이 가능할 경우 취약
- 제거가 불가능한 인터페이스는 비활성화 여부를 확인하고 사후 관리 및 디버깅에 필요한 인터페이스는 접근통제 기능이 적용되어 있는지 확인
- UART 등을 통한 부팅 시점의 로깅 디버깅 메시지 내부에 민감정보(암호화 키 등)가 노출 여부 확인

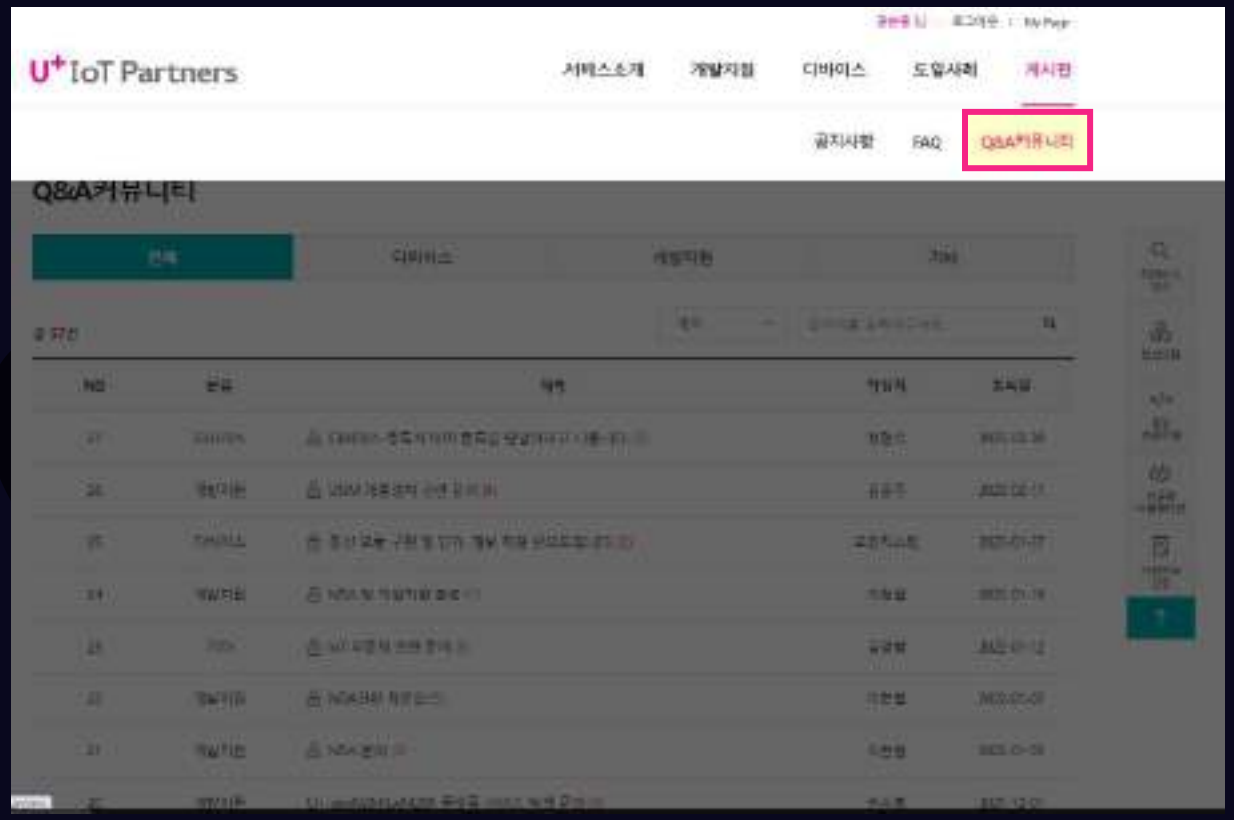
M2M 제휴단말 개발보안 프로세스 및 보안점검 항목

질문 / 답변

01 YouTube 채팅창에 댓글로 질문 등록해 주시면 답변 드리겠습니다. (질문하신 10분은 추첨을 통해 음료쿠폰 발송)

02 향후라도 U+ IoT Partners (https://iotportal.uplus.co.kr) “Q&A커뮤니티” 게시판에 문의를 남겨 주시면 답변 드리겠습니다.

03 Q&A커뮤니티 게시판은 열린 게시판입니다. 공개글은 누구나 볼 수 있으며 댓글을 달 수 있습니다.



Thank you!