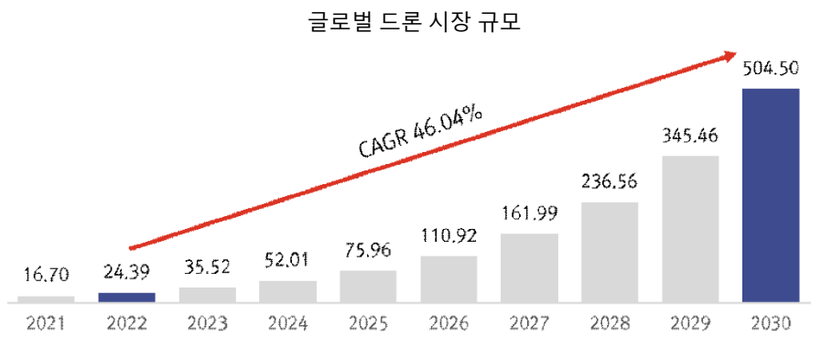
PX4 Autopilot에 대한 보안 취약점 분석

이명진 유승근 차가민 조진성
lumy0726@khu.ac.kr yuu3730@khu.ac.kr gmcha0323@khu.ac.kr chojs@khu.ac.kr
(경희대학교 컴퓨터공학과)

경희대학교 KYUNG HEE UNIVERSITY

■서론

문제 정의



(단위: 십억 달러) 출처: Precedence Research(precedenceresearch.com

드론 발전 흐름에 맞추어 보안 취약점에 대한 지속적인 개선이 필요
오픈소스 SW의 접근성으로 인한 보안 취약점 악용 가능성 증가

PX4 Autopilot 선정하여 연구 진행

연구 방법

- PX4 Autopilot 프로젝트 분석
- 소스 코드 정적 분석
- 결과 분석
- 취약점 재현
- 사전 조사(CVE)
- 알려진 취약점 재현

■연구 결과

소스 코드 정적 분석

CodeQL을 사용한 정적분석 결과 PX4 소스코드 상에서 227 곳의 보안 약점 패턴이 존재

결과 분석

보안 약점 종류가 동일하고 원인의 위치가 같거나 비슷한 것을 합침
131개의 실질적인 보안 약점 정리
소스코드 상에서 확인 후 취약성 추정 결과를 분류

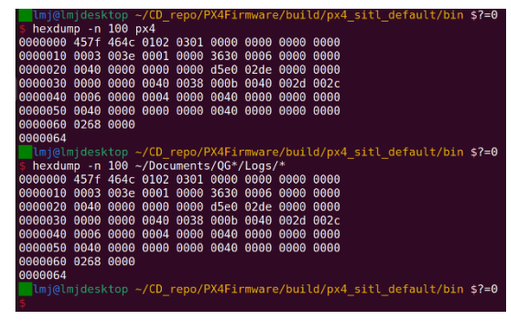
보안 약점 종류	수
계	131
버퍼 길이 오버플로우	12
산술 연산 오버플로우	20
초기화 문제	82
파일 입출력 문제	10
동기화 문제	4
사용자 입력 실행 문제	3

보안 약점 위치	수
계	131
‘./platforms’	12
‘./src/drivers’	10
‘./src/examples’	4
‘./src/lib’	16
‘./src/modules’	85
‘./src/systemcmds’	4

보안 약점 취약성 추정	수
계	131
취약성 확인	3
가능성 높음	3
가능성 낮음	6
가능성 없음	1
확인 불가, 추가분석 필요	76
미 분석	42

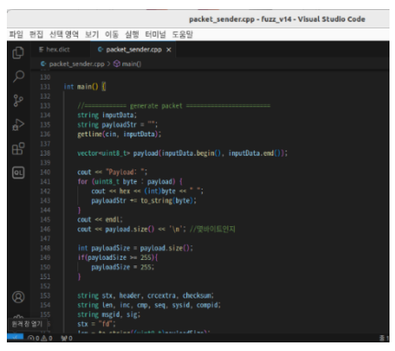
취약점 재현

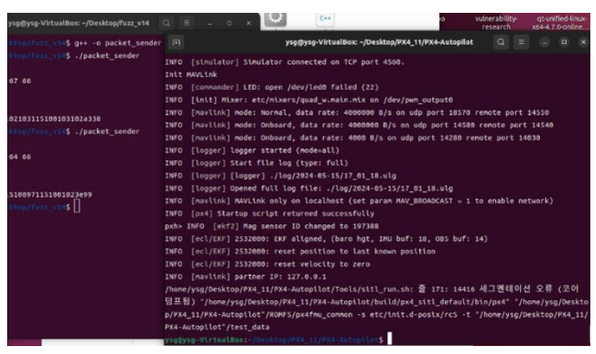
정적 분석 결과에서 exploit할 취약점 선정
mavlink_log_handler.cpp 357번 줄, scanf함수에서 로그의 파일명 읽어오는 과정의 오버플로우 경고
재현 결과 fgets 함수에서 미리 최대 길이 제한됨, 취약성 없음
mavlink_log_handler.cpp 457번 줄, 로그 관리 파일의 권한 지정 없음
외부 공격자가 해당 파일을 쓸 수 있다고 가정하고 공격 진행
QGC에서 수정한 파일명의 파일을 그대로 받아 옴, 취약성 존재



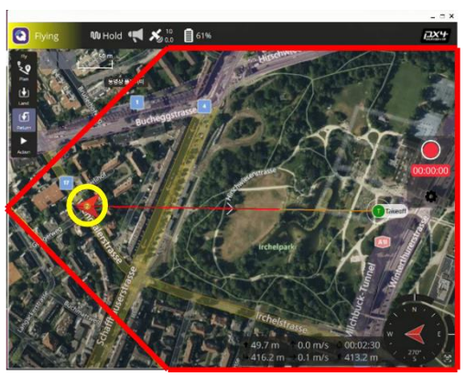
알려진 취약점 재현 (CVE)

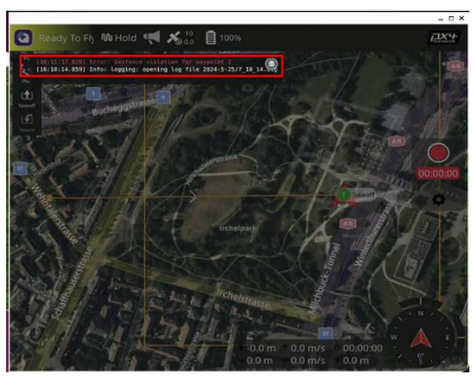
CVE-2021-46896
msgID 332인 MAVLink 패킷으로 오버플로우 발생 가능한 취약점
MAVLink 패킷을 입력으로 받아 14580번 포트에 UDP로 전송하는 코드를 구현
crash를 유발하는 패킷을 입력, 과거 버전인 v1.11.0에서 프로그램이 세그멘테이션 오류와 함께 비정상적으로 종료
비교적 최신인 v1.14.0에서는 취약점 패치가 있어 유효하지 않음





CVE-2024-30800
QGroundControl에서 설정한 geofence 기능을 무시함
비행 중인 드론에 기존 비행금지구역을 허용하는 새로운 mission plan을 다시 업로드
과거 버전인 v1.14.0에서는 경유지가 geofence의 바깥에 있더라도 geofence에 접근할 때까지 비행을 수행함
비교적 최신인 v1.15.0에서는 취약점 패치 완료, 비행 불가





■결론

소스코드 분석을 통해 PX4 Autopilot의 전체적인 동작 흐름과 빌드 과정을 파악
정적 분석을 통해 다수의 취약점 패턴들을 발견, 전제 조건 하 공격 가능한 취약점을 확인
알려진 CVE 취약점은 과거 버전에서 공격 가능, 최신 버전에서 취약점 패치가 이루어짐을 확인

PX4 Autopilot에는 다수의 보안 취약점 존재

보안 취약점의 지속적인 수정이 필요함

소프트웨어 제작 시 잠재적인 보안 약점 주의 필요