기아 K5 IVI 시스템 펌웨어의 공개 취약점 잔존성 분석*

이태훈[01], 조성제[1]
단국대학교 소프트웨어학과[1]
{thththh2015, sjcho}@dankook.ac.kr

Analysis of Residual Public Vulnerabilities in Kia K5 IVI System Firmware

Taehoon Lee[01], Seong-je Cho[1]
Dept. of Software Science[1], Dankook University
{thththh2015, sjcho}@dankook.ac.kr

요 약

최근 차량에 탑재되는 IVI(In-Vehicle Infotainment) 시스템은 내비게이션, 멀티미디어 재생, 스마트폰 연동 등 다양한 편의 기능을 제공하며, USB, 블루투스 등 외부 인터페이스를 통해 사용자와 지속적으로 상호작용한다. 그러나 차량용 IVI 시스템은 일반 모바일 기기나 개인용 컴퓨터에 비해 보안 업데이트 주기가 길고, 패치 적용 과정에서 시스템 재검증 및 배포 절차가 요구되기 때문에 공개 취약점이 장기간 잔존할 가능성이 있다. 본 논문에서는 기아 K5 차량에 탑재된 IVI 시스템 펌웨어를 대상으로 복호화 및 정적 분석을 수행하여 공개 취약점의 잔존 여부를 확인하였다. 분석 결과, Android 미디어 처리 라이브러리인 libstagefright.so에서 CVE-2015-1538 취약점이 패치되지 않은 상태로 존재함을 확인하였다. 해당 취약점은 조작된 MP4 파일의 파싱 과정에서 정수 오버플로우를 유발하고, 이후 힙 오버플로우로 이어질 수 있다. 또한 본 논문에서는 USB 저장장치를 통한 개념적 공격 시나리오를 제시하여, 미디어 파일 자동 파싱 과정에서 사용자의 추가 조작 없이 취약점이 트리거될 수 있음을 이론적으로 분석한다. 본 연구는 차량용 IVI 펌웨어에 공개 취약점이 잔존할 수 있음을 실증적으로 보이고, 차량 소프트웨어 보안 업데이트 및 취약점 관리 체계의 중요성을 제시한다.

1. 서 론

ICT 기술이 차량에 본격적으로 적용되면서 커넥티드 카(Connected Car), 자율주행차량, 소프트웨어 정의 차량(Software-Defined Vehicle, SDV)과 같은 개념이 빠르게 확산되고 있다. 차량은 더 이상 단순한 기계 장치에 머무르지 않고, 다양한 전자제어장치와 소프트웨어를 기반으로 운전자에게 편의 기능과 연결성을 제공하는 복합 시스템으로 발전하고 있다. 특히 IVI(In-Vehicle Infotainment) 시스템은 GPS 내비게이션, 음악 및 동영상 재생, 핸즈프리 통화, 스마트폰 연동 등 운전자와 탑승자가 직접 사용하는 기능을 제공하는 핵심 구성 요소이다.

최근 IVI 시스템은 Android 기반 운영체제를 채택하는 사례가 증가하고 있으며, USB, 블루투스, Wi-Fi, 스마트폰 연동 인터페이스 등 다양한 외부 입력 경로를 통해 사용자와 상호작용한다. 이러한 특성으로 인해 IVI 시스템은 차량 내부 네트워크와 사용자 영역을 연결하는 접점으로 기능할 수 있으며, 보안 취약점이 존재할 경우 공격자가 차량 내부 시스템에 접근하기 위한 초기 침투 지점으로 악용될 가능성이 있다.

일반적인 모바일 기기나 개인용 컴퓨터는 운영체제 및 주요 소프트웨어에 대해 비교적 주기적인 보안 패치를 제공한다. 반면 차량용 IVI 또는 AVN(Audio, Video, Navigation) 시스템은 보안 업데이트 주기가 길고, 패치 적용 과정 또한 상대적으로 복잡하다[1]. 차량 소프트웨어는 코드 수정 이후 기능 안전성, 호환성, 사용자 인터페이스, 차량 내 다른 시스템과의 연동성 등에 대한 재검증이 요구되며[2], OTA(Over-The-Air) 업데이트 인프라가 갖춰지지 않은 차량의 경우 별도의 배포 및 설치 절차가 필요하다. 이러한 제약으로 인해 이미 공개된 취약점이라 하더라도 실제 차량 펌웨어에는 패치되지 않은 상태로 장기간 남아 있을 가능성이 있다.

공개 취약점이 차량용 IVI 시스템에 잔존하는 경우, 공격자는 기존에 알려진 취약점 정보를 기반으로 공격 가능성을 분석할 수 있다. 특히 미디어 파일, USB 저장장치, 블루투스 연결 등 사용자 친화적 기능을 통해 입력되는 데이터가 취약한 라이브러리에서 처리될 경우, 별도의 권한 없이도 취약점이 트리거될 수 있다. 이는 IVI 시스템의 제어권 탈취, 악성 코드 실행, 차량 내부 네트워크 접근 가능성 등으로 이어질 수 있으므로 보안상 중요한 의미를 갖는다.

본 논문에서는 기아 K5 차량의 IVI 시스템 펌웨어를 대상으로 펌웨어 복호화 및 정적 분석을 수행하고, Android 시스템 라이브러리 내에 공개 취약점이 패치되지 않은 상태로 존재하는지를 확인한다. 특히 Android 미디어 처리 라이브러리인 libstagefright.so를 분석하여 CVE-2015-1538 취약점의 잔존 여부를 검증하고, 이를 바탕으로 USB 저장장치를 통한 개념적 공격 시나리오를 제시한다. 본 연구의 목적은 실제 차량용 IVI 펌웨어에서 공개 취약점이 잔존할 수 있음을 보이고, 차량 소프트웨어 업데이트 및 취약점 관리 체계의 필요성을 강조하는 데 있다.

2. 관련 연구

Yan 등[3]은 IVI 펌웨어 추출, 심볼릭 실행, 타겟 퍼징을 결합

* 본 연구는 2024년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업 지원을 받아 수행되었음(2024-0-00035)
이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-학석사연계ICT핵심인재양성 지원을 받아 수행된 연구임(IITP-2026-RS-2023-00259867)

한 계층간 보안 분석 프레임워크를 제안하였다. Mercedes-Benz, Tesla 등 7개 OEM을 대상으로 23개의 취약점을 발견하였으며, 펌웨어에 하드코딩된 자격증명을 통해 원격 차량 제어가 가능함을 시연하였다.

Constantino[4]는 기아의 수출용 차량 CEED의 IVI 앱을 역공학을 수행하여 시스템 앱의 취약점을 분석하였다. 분석 과정에서 엔지니어링 메뉴를 통해 악성 앱을 설치하고 reverse shell을 획득하여 임의 코드 실행 및 CAN 버스 프레임 주입이 가능한 4개의 취약점을 발견하였다. 해당 연구는 실제 동작 중인 기기에 직접 접근하는 분석 방식을 채택하였으며, 앱 레이어를 통한 공격 경로에 초점을 맞추고 있다.

강수영 등[5]은 위협모델링과 공통 평가 기준을 활용하여 IVI 소프트웨어 업데이트 과정에서 발생할 수 있는 보안 위협을 분석하고, 안전한 업데이트를 위한 보안 요구 사항을 도출하였다. 해당 연구는 IVI 시스템의 업데이트 메커니즘에 초점을 맞추어 보안 기준을 제시하였다.

주기호 등[6]은 IVI 시스템의 취약점을 탐지하기 위해 CAN/Ethernet 기반의 퍼징 도구를 개발하고, 차량 내부 네트워크 보호를 위한 IDS를 구현하였다. 해당 연구는 차량 네트워크를 통해 유입되는 외부 공격을 사전에 탐지하는 데 초점을 두었다.

이처럼 IVI 시스템의 펌웨어는 다양한 공격 경로에 노출될 수 있어 보안 위협이 높아, 이를 해소하기 위한 연구가 진행 중이다. 그러나 기존 연구들은 Mazda, Mercedes-Benz, Tesla 및 기아 CEED 등의 해외 중심 차량의 IVI 시스템을 주요 분석 대상으로 삼고 있다. 국내에서는 현대 및 기아 차량이 높은 점유율을 차지하고 있음에도 불구하고, 해당 차량의 IVI 시스템에 대한 보안 분석 연구는 상대적으로 부족하다.

3. 펌웨어 및 취약점 분석

3.1 분석 대상 및 환경

본 논문에서 분석한 차량 및 IVI 시스템 환경은 표 1과 같다. 분석 대상은 2017년식 기아 K5 차량에 탑재된 IVI 시스템이며, 해당 시스템은 Android 4.2.2(Jelly Bean) 기반 운영체제를 사용한다. 분석 대상 펌웨어는 현대/기아 Navigation Updater를 통해 배포되는 최신 내비게이션 업데이트 패키지에서 추출하였다.

표 1. 분석 대상 IVI 시스템 환경

제조 업체	LG Electronics
모델 번호	LAN6420KKJF
펌웨어 버전	JF_17MY.KOR.0.4530.230209.MICOM
소프트웨어 버전	JF_17MY.KOR.SOP.049.241120
OS	Android 4.2.2 (Jelly Bean)
차량	Kia K5(2017)

Android 4.2.2는 비교적 오래된 Android 버전으로, 공개 취약점이 다수 보고된 바 있다. 따라서 본 연구에서는 해당 IVI 시스템의 Android 시스템 파티션에 기존 공개 취약점이 패치되지 않은 상태로 남아 있는지를 중점적으로 확인하였다

3.2 펌웨어 복호화 및 파티션 구조 분석

현대/기아 Navigation Updater를 통해 배포되는 내비게이션 업데이트 패키지에는 IVI 시스템 업데이트를 위한 펌웨어 파일이 포함되어 있다. 본 연구에서 분석한 펌웨어 파일은 upgrade.lgk 이며, 해당 파일은 AES-128-CTR 모드로 암호화되어 있었다. 또한 암호화 키는 KEK(Key Encryption Key)와 마스터 키를 사용하는 이중 구조로 관리되는 것을 확인하였다.

표 2. 복호화된 펌웨어 내부 파티션 구성

파티션	명칭	설명
P0	recovery	시스템 복구 파티션
P1	bootloader	부트로더 바이너리
P2	bootimg	부트 이미지
P3	system	Android 시스템
P4	snapshot	시스템 스냅샷
P5	snapshot2	시스템 스냅샷
P6	micom	마이컴 파티션

본 논문에서는 펌웨어 암호화 구조를 분석하여 upgrade.lgk 파일을 복호화하고, 내부에 포함된 파티션 구성을 확인하였다. 복호화된 펌웨어는 여러 파티션으로 구성되어 있었으며, 그중 Android 시스템 파티션은 운영체제 라이브러리와 실행 파일을 포함하고 있어 취약점 분석의 주요 대상이 된다. 표 2는 복호화 후 확인한 내부 파티션 구성을 나타낸다. 본 논문에서는 Android 시스템 파티션을 대상으로 정적 분석을 수행하였다. 특히 Android 미디어 처리 과정에서 사용되는 시스템 라이브러리를 중심으로, 기존에 공개된 취약점이 패치되었는지 여부를 분석하였다.

3.3 Android 시스템 라이브러리 취약점 분석

Android 4.2.2에서 보고된 공개 취약점들이 차량 IVI 펌웨어에도 존재하는지 확인하기 위해, 복호화된 Android 시스템 파티션을 대상으로 정적 분석을 수행하였다. 분석에는 바이너리 분석 도구인 Ghidra를 사용하였으며, Android 시스템에서 라이브러리 폴더 중 미디어 파일 파싱과 관련된 libstagefright.so를 중점적으로 분석하였다.

분석 결과, libstagefright.so에서 CVE-2015-1538 취약점이 패치되지 않은 상태로 존재함을 확인하였다. CVE-2015-1538은 Android 미디어 처리 라이브러리의 MP4 파일 파싱 과정에서 발생하는 취약점으로, 조작된 MP4 파일 내 특정 atom 값을 처리하는 과정에서 정수 오버플로우가 발생하고, 이후 힙 오버플로우로 이어질 수 있다[7]. 해당 취약점은 미디어 파일 파싱 과정에서 발생하므로, 사용자가 직접 파일을 실행하지 않더라도 시스템의 미디어 스캐닝 과정에서 취약 코드가 호출될 가능성이 있다.

Ghidra를 이용한 정적 분석 결과, MP4 파일의 stsc atom을 파싱하는 함수가 내부적으로 샘플 테이블 관련 파라미터를 설정하는 함수를 호출하는 경로를 확인하였다. 이 과정에서 entry_count 값을 기반으로 버퍼 크기를 계산하는 연산이 수행되며, 특정 조건에서 정수 오버플로우가 발생할 수 있음을 확인하였다. 오버플로우가 발생한 연산 결과가 힙 버퍼 할당 크기로 사용될 경우, 실제 필요한 크기보다 작은 버퍼가 할당될 수 있다. 이후 원래의 entry_count 값을 기준으로 반복적인 쓰기 작업이 수행되면, 할당된 버퍼 범위를 초과하는 힙 오버플로우가 발생할 수 있다.

본 논문에서는 취약점의 존재 여부와 발생 원리를 정적 분석을 통해 확인하였으며, 실제 악용 코드나 공격 페이로드는 보안 및 윤리적 이유로 제시하지 않는다.

4. USB 기반 개념적 공격 시나리오

본 장에서는 3장에서 식별한 CVE-2015-1538 취약점을 기반으로, 실제 차량 환경에서 공격이 전개될 수 있는 가능성을 개념적으로 분석한다. 본 시나리오는 취약점의 악용 가능성을 설명하기 위한 이론적 분석이며, 실제 공격 코드나 재현 가능한 페이로드는 포함하지 않는다.

그림 1은 조작된 MP4 파일을 이용한 USB 기반 공격 흐름을 나타낸다. 공격자는 취약점을 유발할 수 있는 MP4 파일을 제작하여 웹사이트, 메신저, 파일 공유 서비스 등 일반적인 경로를

통해 배포할 수 있다. 차량 소유자가 해당 파일을 USB 저장장치에 저장한 뒤 IVI 시스템에 삽입하면, IVI 시스템은 USB 내 미디어 파일을 인식하고 자동으로 미디어 스캔을 수행한다.

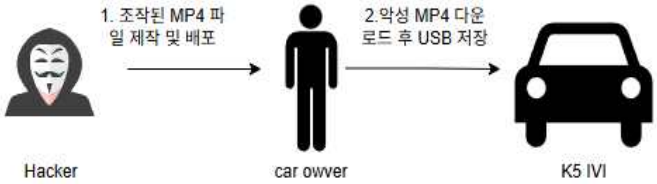

그림 1. 조작된 MP4 파일을 이용한 USB 기반 공격 흐름

Android의 MediaScanner는 저장장치 내 MP4 파일의 메타데이터를 확인하기 위해 미디어 처리 라이브러리인 libstagefright.so를 호출한다. 이 과정은 사용자가 파일을 직접 재생하지 않더라도 자동으로 수행될 수 있으므로, 미디어 파일 파싱 기능은 IVI 시스템의 주요 공격 표면이 될 수 있다(그림 2 참조).

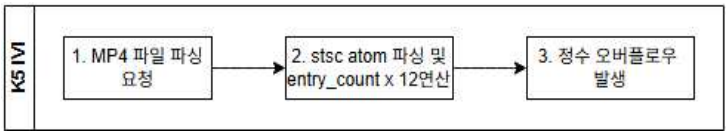

그림 2. USB 삽입 후 IVI 내부의 취약점 트리거 흐름

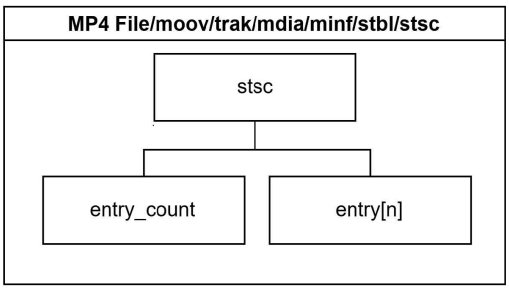

그림 3. MP4 파일의 구조 및 stsc

MP4 파일은 여러 atom으로 구성되며, 각 atom은 파일의 메타데이터, 트랙 정보, 샘플 정보 등을 표현한다. 그림 3은 MP4 파일 구조의 개념도를 나타낸다. CVE-2015-1538 취약점은 MP4 파일의 stsc atom을 처리하는 과정에서 발생한다. libstagefright.so는 entry_count 값을 기반으로 버퍼 크기를 계산하는데, 이 값이 비정상적으로 클 경우 곱셈 연산에서 정수 오버플로우가 발생할 수 있다. 그 결과 실제 필요한 크기보다 작은 힙 버퍼가 할당되고, 이후 기존 entry_count 값을 기준으로 반복적인 쓰기 작업이 수행되면서 힙 오버플로우가 발생할 수 있다.

이러한 힙 오버플로우는 프로세스 비정상 종료, 메모리 손상, 실행 흐름 변조 가능성으로 이어질 수 있다. 본 분석은 차량용 IVI 시스템에 공개 취약점이 잔존할 경우, USB 저장장치와 같은 일반적인 사용자 인터페이스가 공격 경로로 악용될 수 있음을 보여준다. 따라서 IVI 펌웨어에 대한 정기적인 취약점 점검과 보안 업데이트 체계가 필요하다.

제시한 공격 시나리오 기반 분석은 차량용 IVI 시스템에서 미디어 파일 자동 파싱 기능이 공격 표면으로 작용할 수 있음을 보여주며, 펌웨어 내 공개 취약점 제거와 정기적인 보안 업데이트 체계 구축의 필요성을 시사한다.

5. 결론 및 한계점

본 논문에서는 K5 2017 IVI에 들어가는 펌웨어를 복호화하여 내부 파티션을 분석하였으며 Android 4.2.2 기반의 시스템의 취약점이었던 CVE-2015-1538이 패치되지 않은 상태로 존재하는 것을 확인하였다. 해당 취약점은 조작된 MP4 파일만으로 사용자 상호작용 없이 정수 오버플로우를 유발할 수 있으며 힙 오버플로우로 이어질 수 있는 잠재적 공격 경로를 가지고 있다. OTA 업데이트를 지원하지 않는 차량의 경우, 최신 펌웨어에도 레거시 OS 취약점이 존재함을 보여주며, OTA 미지원 차량에 대한 별도의 보안 관리 체계가 필요하다.

근본적인 해결책은 CVE-2015-1538에 대한 보안 패치 적용이지만, 높은 비용과 복잡한 배포 과정을 수반한다. 효과적 대응 방안으로 USB 삽입 시 MP4 파일의 접근을 차단하는 미디어 파일 필터링 기법을 적용할 수 있다. 본 논문에서 정적 분석을 통해 IVI 펌웨어 코드 수준의 취약점을 확인하였으며, 향후 연구에서는 실제 환경에서의 동작 검증 및 추가적인 공격 경로 분석이 필요하다.

참고 문헌

[1] 김주성, "자동차 소프트웨어 생태계 관련 주요 이슈 및 발전방안", 전자통신동향분석, 38, 5, 82-89, 2023

[2] Jaewan Seo et al., "Development for High-Assurance Software Update Management System Complying With UN R156", IEEE Access, 12, (no issue), 135811-135830, 2024.

[3] M. Yan, G. Crane, D. Suillivan, and H. Shan, "Driving into the Unknown: Investigating and Addressing Security Breaches in Vehicle Infotainment Systems," Sensors, Vol.26, No.1, pp.77, 2026.

[4] G. Costantino and I. Matteucci, "Reversing Kia Motors Head Unit to discover and exploit software vulnerabilities," Journal of Computer Virology and Hacking Techniques, Vol.19, pp.33-49, 2023.

[5] 강수영, 김승주, "위협모델링과 공통평가기준을 활용한 인포테인먼트의 안전한 업데이트 보안요구사항 분석," 정보보호학회논문지, Vol.29, No.3, pp.613-623, 2019.

[6] 주기호 외, "차량 보안 취약점 분석 도구 개발 및 네트워크와 제어기 보호를 위한 IDS 개발," 과학기술정보통신부 최종보고서, 과제번호 2022-0-00023, 2024.

[7] J. J. Drake, "Stagefright: Scary Code in the Heart of Android," in Proc. Black Hat USA 2015, USA, Aug. 2015.