드론 환경에서의 FTP 및 텔넷 접속 취약점 분석 및 실증: A 드론을 대상으로

오경석*, 정원빈O, 이재혁**, 이경률*
*목포대학교 정보보호학과,
O목포대학교 정보보호학과,
**목포대학교 정보보호기술학협동과정
e-mail: {gin3724*, goblebinO, gurtmggg**}@mokpo.ac.kr, carpedm@mnu.ac.kr*

Vulnerability Analysis and Demonstration of FTP and Telnet Access in Drone Environment: Based on Product A

Gyeongseok Oh*, Wonbin JeongO, Jaehyuk Lee**, Kyungroul Lee*
*Dept. of Information Security Engineering, Mokpo National University,
ODept. of Information Security Engineering, Mokpo National University,
**Interdisciplinary Program of Information & Protection, Mokpo National University

● 요 약 ●

드론 기술이 발전함에 따라, 최근에는 재난 구조 및 교통 관측, 과학 연구와 같은 분야에서 드론이 활용됨으로써, 사회적 및 산업적 발전에 일조하는 실정이다. 그러나 드론의 사용률이 증가하는 상황에서, 다양한 취약점을 내포한 드론으로 인하여, 심각한 보안위협이 발생하는 문제점이 존재한다. 이에 따라, 드론에서 발생하는 보안위협에 대응하기 위한 연구가 요구되며, 본 논문은 대응방안을 도출하기 위한 목적으로, 드론에서 발생 가능한 신규 취약점을 분석하고 실증한다. 본 논문에서 발굴한 신규 취약점은 A 드론을 대상으로, 기존의 다중 접속 취약점을 악용한 FTP 및 TELNET 접속 취약점이며, FTP 접속으로 암호화된 파일에 접근이 가능하고 TELNET 접속으로 루트 권한의 셸을 실행하는 신규 취약점을 발굴하였다.

키워드: 드론(drone), 취약점 분석(vulnerability analysis), 텔넷(telnet)

I. 서론

주로 군사용 목적으로 개발되었던 드론 기술은 최근 대중화 목적으로 개발됨에 따라, 재난 구조, 교통 관측, 과학 기술과 같은 다양한 서비스와 연계하여, 사회적 및 산업적 발전에 기여하고 있다[1]. 이와 같이, 다양한 서비스를 제공함으로써, 드론의 사용률이 증가함에 따라, 드론 제조사에서는 드론에서 발생 가능한 취약점에 대응하기 위하여 다양한 보안 기능을 적용하였으며, 대표적인 보안 기능은 인가된 사용자를 제외한 비인가된 사용자로부터의 드론 접속을 차단하기 위하여, 연결 가능한 기기의 개수를 제한하는 기능이다.

그러나 이러한 보안 기능이 적용되었음에도 불구하고, 알려지지 않은 다양한 취약점이 내포됨에 따라, 추가적인 보안위협이 발생할 가능성이 존재한다[2]. 따라서 본 논문에서는 드론에서 발생하는 보안위협에 대응하기 위한 방안을 도출하기 위한 목적으로, A 드론을 대상으로, 기존의 다중 접속 취약점을 악용한 FTP(File Transfer Protocol) 및 TELNET 접속과 관련된 신규 취약점을 분석하고 실증한다.

II. 신규 취약점 발생 가능성 분석

선행 연구인 A 드론의 다중 접속 취약점을 살펴보면, A 드론은 연결 가능한 기기의 개수를 제한하는 기능이 적용되어 있음에도 불구하고, 설정 파일을 변조함으로써, 연결 가능한 기기의 개수를 초과하여 다중 접속이 가능함을 실증하였다[2]. 본 논문에서는 이와 같은 다중 접속 취약점을 악용하여, A 드론에서 발생 가능한 추가적인 취약점을 분석한다. 추가적인 취약점을 분석하기 위하여, 드론에 접속한 공격자가 드론 내부로 침투하는 과정이 필요할 것으로 판단하였으며, 열린 포트를 스캔한 결과와 셸 접근 가능성을 분석하였다.

1. 포트 스캔 결과 및 FTP 취약점 분석

우선, 공격자 입장에서 드론 내부로 침투하기 위하여, 열린 포트를 확인하였으며, NMAP(Network MAPper) 도구를 사용하여 스캔한 결과를 표 1에 나타내었다.

Table 1. A 드론의 포트 스캔 결과

열린 포트 번호	서비스
21	FTP
67	DHCP
5037	드론과 조종기 간 통신 포트로 추정
9003	드론과 조종기 간 통신 포트로 추정

표를 살펴보면, A 드론은 4개의 포트가 열려있었으며, 그중, 5037번 포트와 9003번 포트는 드론과 조종기 간 통신에 사용되는 포트로 추정되고, 67번 포트는 조종을 위하여 접속한 단말에 동적으로 IP(Internet Protocol) 주소를 할당하는 DHCP(Dynamic Host Configuration Protocol) 서버를 위한 포트이다. 마지막으로 21번 포트는 FTP 서버로, 드론에서 촬영하여 저장한 사진이나 영상 파일에 접근하기 위한 용도로 활용된다.

본 논문에서는 열린 포트 중, 21번 포트인 FTP에 접속하여, 촬영된 사진이나 영상 파일의 탈취 가능성을 분석하였으며, 그 결과, 드론의 모든 디렉터리에는 접속할 수 없고 일부 디렉터리에만 접근이 가능하였다. 그뿐만 아니라, 접근 가능한 일부 디렉터리에 저장된 대부분의 파일은 암호화되어, 공격자의 입장에서 드론 내부에 저장된 민감한 정보를 탈취하기에는 한계점이 있는 것으로 판단된다.

2. ADB 접속을 통한 신규 취약점 분석

상기와 같은 이유로, 열린 포트를 통하여 추가적인 취약점이 발생하지 않는 것으로 판단되어, ADB(Android Debug Bridge)로 접속하여, 신규 취약점의 발생 가능성을 분석하였다. ADB 접속을 위하여, DUMLdore 도구를 사용하여 유선으로 루트셸을 실행하였으며, 루트 권한으로 현재에는 제공하지 않는 TELNET 서비스를 시작할 수 있을 것으로 분석하였다. 결국, 공격자는 TELNET 서비스를 시작함으로써, 원격으로 드론에서 제공하는 셸에 접속할 수 있으며, 셸 접속을 통한 추가적인 취약점을 발굴할 수 있을 것으로 판단된다.

III. TELNET 접속 취약점 실증

공격자의 입장에서 TELNET에 접속하기 위하여, ADB 접속으로 루트셸을 획득한 후, TELNET 서비스를 강제로 시작하였으며, 서비스가 정상적으로 제공되는지 확인하기 위하여, 그림 1과 같이 netstat 명령으로 열린 포트를 확인하였다.

```
root@wm100_dz_ap0001_v5:/ # busybox telnetd -l /system/bin/sh
root@wm100_dz_ap0001_v5:/ # netstat
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:9003            0.0.0.0:*               CLOSE
```

Fig. 1. TELNET 서비스 강제 시작 및 열린 포트 확인

확인 결과, 그림과 같이, TELNET 서비스가 정상적으로 시작되었고, 23번 포트가 열린 것을 확인하였다. 이를 통하여, 공격자가 원격으로 TELNET 접속이 가능할 것으로 판단하였으며, TELNET에 접속한 결과, 그림 2와 같이, 루트 권한으로 셸이 실행된 것을 확인할 수 있다. 이후, 공격자는 루트 권한으로 파일을 열람하거나 수정, 삭제와 같은 악의적인 행위가 가능할 것으로 사료된다.

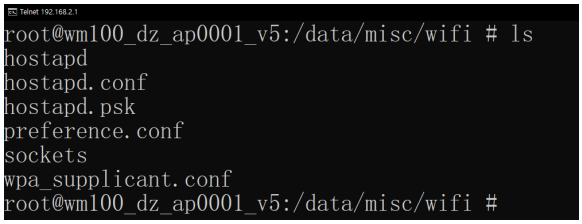

Fig. 2. TELNET 접속 결과

IV. 결론

본 논문은 무선 네트워크를 사용하는 A 드론을 대상으로, 선행 연구인 다중 접속 취약점을 악용하여, 추가적으로 발생 가능한 신규 취약점을 발굴하였다. 발굴한 신규 취약점은 ADB 접속을 통하여 TELNET 서비스를 강제로 시작하여, 루트 권한의 셸을 실행하는 취약점이며, 공격자가 루트 권한을 탈취함으로써, 드론의 모든 제어권을 확보하는 심각한 취약점을 실증하였다. 향후, 본 논문에서 실증한 결과를 기반으로, 추가적으로 발생 가능한 신규 취약점을 분석하고, 대응방안을 도출하는 연구를 진행할 예정이다.

ACKNOWLEDGEMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2021R1F1A1050542, NRF-2021R1A4A2001810).

REFERENCES

[1] J. Jin and G. Lee, "Understanding and Trends in UAVs/Drone," Journal of Korean Institute of Communications and Information Sciences, Vol. 33, No. 2, pp. 80-85, Jan. 2016.

[2] G. Oh, J. Lee, and K. Lee, "Multiple Access Vulnerability Analysis of Wireless Network: Based on Drone A Product," Proceedings of the 15th Workshop on Convergent and Smart Media Systems, Feb. 2023.

[3] DumLdore, https://github.com/jezzab/DUMLdore, Retrieved from 26 Jun. 2023.