# Analysis and Systematization of Vulnerabilities of Drone Subsystems

Maryna Kolisnyk and Oleksandr Piskachov

August 15, 2023

# Analysis and systematization of vulnerabilities of drone subsystems

Kolisnyk Maryna and Piskachov Oleksandr

National Aerospace University "Kharkiv Aviation Institute"
m.kolisnyk@csn.khai.edu

**Abstract.** A drone is a software (SW) and hardware (HW) complex that has wireless data transfer technologies (Wi-Fi, LTE, 5G, Bluetooth, etc.) To transfer data, it uses various communication protocols: both specific and generally known.

Drones can perform complex tasks, but some cyber-attacks (such as Denial-of-Services - DoS) can lead to the failure of individual components of the drone and the entire system as a whole.

Guidelines for protecting against drone attacks are provided by many organizations that develop cybersecurity standards (NIST, CERT, CISA, etc.). Measures to prevent cyber-attacks can be applied to drones, with some adjustments to their parameters and architectural features. There are also recommendations for protecting drone components and also methods of communication protocols protection from cyber-attacks.

The authors of this study offer a comprehensive approach to the analysis of vulnerabilities of drone subsystems, which includes a system analysis of drone architecture, vulnerability analysis by different vulnerability databases, and their systematization.

**Keywords:** Vulnerabilities, Drone, System Analysis, Cyber-Attacks.

## 1 Introduction

### 1.1 Motivation and Relevance of Research

Drones can use digital protocols and embedded systems such as I2C, SPI, Serial, CAN, 1-wire, etc. Flight controllers used in UAVs are usually built using popular microcontrollers such as: Atmega, STM (ARM), Intel Movidius, sometimes low-voltage Intel/AMD x86/x64 microcontrollers (Fig. X.1) [1], [2].

Drones use communication protocols, operating systems (OS), hardware (HW) in the control device of the drone is similar to other digital systems. Therefore, drones can be affected by cyber-attacks that use the vulnerabilities of these HW and SW subsystems of the drone in their mechanisms.

The scientific novelty of the obtained results lies in the fact that, based on the system analysis of the architecture of drones, the paper will perform an analysis of the vulnerabilities of their HW and SW subsystems, and their systematization according to the types of cyber-attacks.

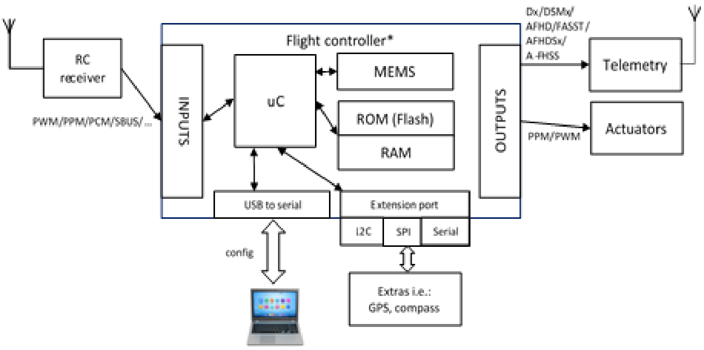


**Fig. 1.** The structure scheme of drone according to [1]

The practical significance of the obtained results is that the systematization of drone vulnerabilities according to the types of cyber-attacks will allow us to propose a method of prioritizing drone's vulnerabilities and a method of assessing and ensuring their dependability, which will increase the reliability and cybersecurity of drones.

### 1.2 Work Related Analysis

The issue of cyber security of drones is very relevant, especially during military operations. There are publications about communication methods and cybersecurity issues of drones. The report [1] describes decisions to organize secured and resilient transparent IP access to drones / ground station (using both LTE and Wi-Fi technologies). In the paper [2] was described a high-level architecture multi-drone system consisting of quadrotors for the design of a collaborative aerial system that consists of drones with on-board sensors and embedded processing, sensing, coordination, and communication and networking capabilities with different conditions and impact factors. The videostream of the drone is interest for a potential attacker due to its ability of revealing confidential information. A security threat analysis on this particular drone and use-case, how the drone can be hacked in order to hijack the AR.Drone 2.0 were proposed in the paper [3]. In paper [4], were presented general challenges in the deployment of UAV and comparison of UAV communication services based on its operating frequency, major collision avoidance approaches, were discussed collision avoidance approaches that are suitable for indoor applications, was presented the Flying Adhoc Networks (FANET) network architecture, communication and routing protocols for each Open System Interconnection (OSI) communication layers. The paper [5] presents some networking protocols for the UAV wireless networks. The paper [6] proposes a Drone enabled Data Communication for Internet of Things (DDC-IoT) as a data communication solution for IoT networks, data collection centers and drones, which was tested in simulation to analyze its performance especially for real time critical applications in terms of data throughput and data delay. In [7] was analyzed the vulnerability of the micro air vehicle communication (MAVLink) protocol for GCS-based control of UAVs and an attack methodology that can disable an ongoing mission of a UAV was proposed. An encryption technique is proposed in [8], that makes the communication between the UAV and GCS secure, based on the analysis of MAVlink protocol vulnerabilities.

Since a drone is a complex HW and software (SW) device that connects to the Internet using appropriate data transmission technologies, it can be considered one of the network devices. And this means that it can be affected by all types of cyber attacks that operate in a regular computer network [9], [10]. Similar measures to prevent cyber-attacks can be applied, with some amendments to the parameters and features of the drone structure. There are many organizations (NIST, CERT, etc.) offering guidance on how to defend against drone vulnerability attacks. There are also guidelines for protecting drone components and the communication protocols they use to transmit data separately from cyber-attacks. The authors of this study offer a comprehensive approach to analyzing the vulnerabilities of drone subsystems, based on their systematization.

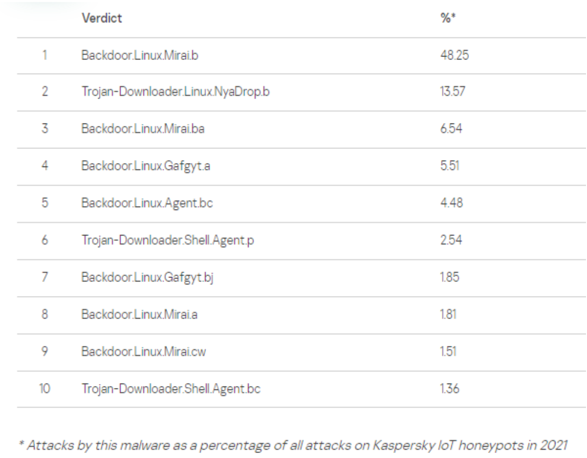
The purpose of this study: analysis and systematization of the most serious vulnerabilities of drone subsystems and cyber-attacks that can affect them, and recommendations for their prevention, detection and mitigation.

## 2 Analysis of drone’s subsystems vulnerabilities

### 2.1 Vulnerabilities in the OS

The correct performance of drone tasks depends on the correct functioning of the OS. Quite often, microcontrollers and drone processors use the Linux OS. The report of Kaspersky Lab from 2021 indicates a large number of cyber-attacks specifically on the Linux OS (Fig. 2) [11].

EvilGnome spyware [12], [13] which is currently not included in all major antivirus security SW products, including features rare to most Linux malware. In the Linux kernel, a vulnerability signed in the National Vulnerability Database (NVD) as CVE-2020-14314, an out-of-memory read vulnerability was discovered in a way to access a wrongly indexed directory [14]. This vulnerability could allow a local user to crash the system if the directory exists and compromise system availability. Over the past 2 years, about 50 vulnerabilities of varying degrees of severity have been discovered in the Linux OS. According to the Linux OS Vulnerability Database, CVE-2020-16119 was discovered when the DCP protocol was injected into the OS kernel, leading to a Denial of Service (DoS) attack (destruction of the OS) or the ability to execute malicious code, and vulnerable places lead to such consequences [15], [16].



| | Verdict | %* |
|---|---|---|
| 1 | Backdoor.Linux.Mirai.b | 48.25 |
| 2 | Trojan-Downloader.Linux.NyaDrop.b | 13.57 |
| 3 | Backdoor.Linux.Mirai.ba | 6.54 |
| 4 | Backdoor.Linux.Gafgyt.a | 5.51 |
| 5 | Backdoor.Linux.Agent.bc | 4.48 |
| 6 | Trojan-Downloader.Shell.Agent.p | 2.54 |
| 7 | Backdoor.Linux.Gafgyt.bj | 1.85 |
| 8 | Backdoor.Linux.Mirai.a | 1.81 |
| 9 | Backdoor.Linux.Mirai.cw | 1.51 |
| 10 | Trojan-Downloader.Shell.Agent.bc | 1.36 |

** Attacks by this malware as a percentage of all attacks on Kaspersky IoT honeypots in 2021*

**Fig. 2.** Statistics of cyber-attacks on Linux OS in 2021 [11]

Vulnerabilities CVE-2020-14314 and CVE-2020-16120, CVE-2020-14385, CVE-2020-20285, CVE-2020-25641 help an attacker to perform successful DoS attacks. Many malware targeting Linux OS mainly focus on attacks to create DoS botnets by hijacking vulnerable servers [14], [17]-[20]. The latest vulnerability of 2022 - CVE-2022-23222 in the Linux kernel with severity level 7.2 allows local users to gain privileges [21]. There is a risk of complete disclosure of information, as a result of which all system files are disclosed, a complete violation of the integrity of the system occurs. There is a complete loss of protection of the entire system and a complete shutdown of the affected resource. An attacker can make a resource completely unavailable; there are no special access conditions or mitigating circumstances. Using the vulnerability does not require authentication and additional knowledge or skills. A large number of malware targeting Linux mainly focus on attacks to create DoS botnets by hijacking vulnerable servers. CVE-2022-2873 [22] - an out-of-bounds memory access flaw was found in the Linux kernel Intel's iSMT SMBus host controller driver I2C_SMBUS_BLOCK_DATA with malicious input data, and the such flaw allows a local user to crash the system (DoS ). CVE-2023-2194 out-of-bounds vulnerability was found in the Linux kernel's SLIMpro I2C device driver and could allow a local privileged user to crash the system (DoS) or potentially achieve remote code execution [23]. If the firewall in the OS fails, the risk of a successful attack on the drone increases, as a malfunctioning OS can cause the drone's systems to fail. The drone works with a large number of communication protocols, such as: Hypertext Transfer Protocol (HTTP), Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP) and MQ Telemetry Protocol (MQTT). Discovery and Configuration Protocol (DCP), SSH File Transfer Protocol (SFTP), VPN, Simple Network Time Protocol (SNTP), Simple Network Management Protocol (SNMP), Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), Secure Shell Protocol (SSH), Network Time Protocol (NTP), Real-time Transport Protocol (RTP), Real-time control Protocol

(RTCP). Vulnerabilities in these protocols can lead to a successful attack on drone subsystems.

### 2.2 Vulnerabilities in the SSH Protocol

Over 39 SSH vulnerabilities led to successful cyberattacks in 2022: Stored Cross-Site Scripting (XSS) Vulnerability Exploitable by an Attacker with General/Administrator Permissions (3 Vulnerabilities), DoS (11 Vulnerabilities), CSRF (4 Vulnerabilities), Remote Code Execution (7 vulnerabilities) (Fig. 3). CSRF vulnerability in Jenkins publisher plugin SCP 1.8 and earlier allows attackers to connect to an attacker-specified SSH server using attacker-specified credentials. In 2021, CVE-2021-1378 [24], [25] and CVE-2021-1592 [26] were exposed, vulnerabilities in the Cisco StarOS SSH service that could allow an unauthenticated remote attacker to cause an affected device to stop processing traffic leading to a DoS condition. The vulnerability is related to a logic error that can occur under certain traffic conditions. An attacker could exploit this vulnerability by sending a series of crafted packets to an affected device. A successful exploit could allow an attacker to prevent the target service from receiving any traffic, resulting in a DoS condition on the affected device.

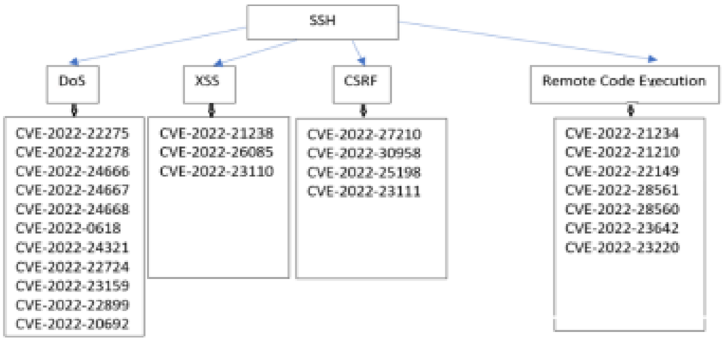


**Fig. 3.** Vulnerabilities in the SSH protocol

### 2.3 Vulnerabilities in the NTP protocol

Network Time Protocol (NTP) is a network protocol for synchronizing the clocks of all servers and clients, used in drones. The NTP protocol has been found to be vulnerable to a number of attacks. The most frequently used were command injection (8 vulnerabilities in 2020-2022), XSS (2 vulnerabilities in 2020), DoS (3 vulnerabilities in 2020-2021). In 2022, vulnerabilities that facilitate brute force attacks (1 vulnerability) and remote command execution (3 vulnerabilities) appeared (Fig. 4).

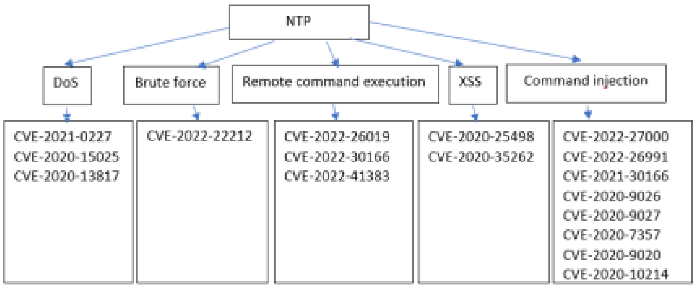


**Fig. 4.** Vulnerabilities of the NTP protocol

Several vulnerabilities led to successful DoS-attacks: CVE-2020-15025 allows remote attackers to cause DoS (memory consumption) [27]; CVE-2020-13817 [28] allows remote attackers to cause a DoS of drone (modification of system time or denial of service) by predicting transmission timestamps for use in forged packets; CVE-2020-11868 [29] - NTP is vulnerable to DoS; CVE-2022-27000 [30] allows attackers to execute arbitrary commands via a crafted request; CVE-2022-26019 [31] - improper access control vulnerability allows a remote, privileged attacker to modify NTP GPS settings to overwrite existing files on the file system, which could lead to arbitrary command execution.

### 2.4 Real Time Protocol (RTP) Vulnerabilities

CVE-2018-0280 [32] Real-Time Transport Protocol (RTP) bitstream processing vulnerability in Cisco Meeting Server allows an unauthenticated remote attacker to cause a DoS condition by sending a crafted RTP bitstream to an affected Cisco Meeting Server (when transmission of information from a drone). This leads to the failure of audio and video services, failures in the media process, which will lead to a DoS state on the affected product.

### 2.5 Real-time Control Protocol (RTCP) Vulnerabilities

When operating the drone with PJSIP, a free and open-source multimedia communications library written in C that implements standard protocols such as SIP, SDP, RTP, STUN, TURN, and ICE, there are various cases where some incoming RTP/RTCP packets can potentially cause out-of-bounds read access. In the NVD database, this is the vulnerability CVE-2022-21722 [33]. It applies to all users who use PJMEDIA and receive incoming calls RTP/RTCP.

### 2.6 VPN Vulnerabilities

The use of VPNs to improve drone cybersecurity has been proposed by several research groups (рис. 5) [34].

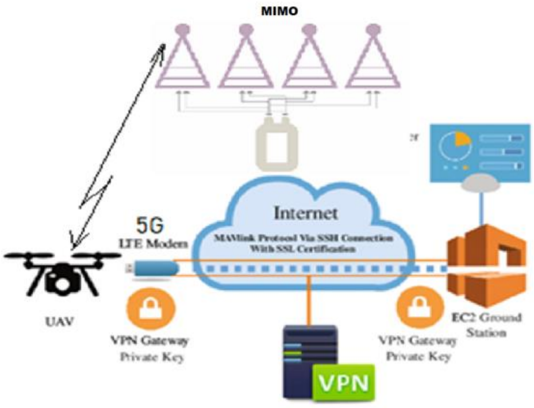


**Fig. 5.** Scheme of VPN implementation between drones according to [34]

In 2022 alone, 21 VPN vulnerabilities have already been identified that can lead to various types of cyber-attacks, including DoS. VPNs are dangerous because they expose entire networks to threats such as malware, DDoS-attacks, and spoofing-attacks. Once an attacker penetrates a network through a compromised device, the entire network can be destroyed [34]-[36]. The most common vulnerabilities in 2022 that led to cyber-attacks were: DoS (7 vulnerabilities in 2020), SQL injection (1 vulnerability), Man-in-the-Middle (1 vulnerability), Buffer overflow (1 vulnerability), XSS (1 vulnerability), implementation of OS arguments and commands (3 vulnerabilities) (Fig. 6).

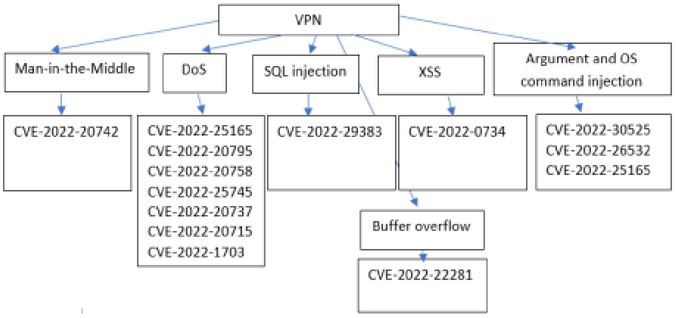


**Fig. 6.** Vulnerabilities in VPN in 2022

## 2.7 Random Access Memory (RAM) Vulnerabilities

It is known that a dynamic memory cell uses a capacitor and 3 transistors to store one bit of information. Capacitors lose charge over time, and a stored bit value of "1" (which may indicate a high charge) may change to a "0" (low charge). However, every time a row of memory is activated for reading or writing (the bits are staggered in rows and columns), currents flowing inside the chip can cause the capacitors to discharge. The charge will flow faster in adjacent rows. This means that by re-activating—or "injecting"—a row of memory (the "aggressor"), an attacker can cause bit errors in an adjacent row, also called a "victim" row. This bit error can be used to give attackers access to restricted areas of a computer system without relying on any software vulnerability. The vulnerability, called Rowhammer, is a design flaw in the device's internal memory (DRAM) chips that creates a vulnerability that could allow an attacker to gain control of the drone.

## 2.8 Vulnerabilities in the SNMP Protocol

In 2022, a serious vulnerability appeared in the SNMP protocol [37], [38], which leads to the failure of the drone when a DoS-attack is successfully implemented. In total, 5 protocol vulnerabilities were identified that can lead to successful DoS-attacks (Fig. 7).

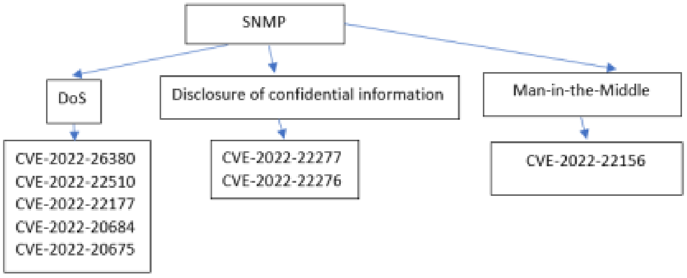


**Fig. 7.** Vulnerabilities in the protocol SNMP

## 2.9 Vulnerabilities in the MQTT Protocol

Vulnerabilities of the MQTT, CoAP protocols can be used to organize espionage, targeted attacks, intelligence by attackers [39]. An attacker can scan and gain access to vulnerable MQTT peripherals such as drones using IP web scanners and gain access to these devices. Also, an unusual cache-hit vulnerability was discovered in this protocol: CVE-2022-0673 [40] — external schema file cache poisoning via directory traversal. The highest number of MQTT protocol vulnerabilities were exploited by attackers in 2022 and 2021 for successful DoS attacks (3 vulnerabilities), SSRF (1 vulnerability), Man-in-the-Middle (2 vulnerabilities), remote code execution (7 vulnerabilities) (Fig. 8).

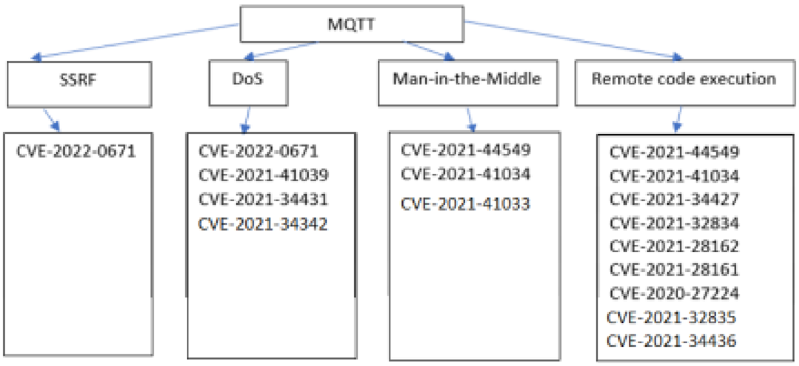


**Fig. 8.** Vulnerabilities in the protocol MQTT

### 2.10 Vulnerabilities in the CoAP Protocol

CVE-2020-3162 [41] - a vulnerability in the Constrained Application Protocol (CoAP) implementation of Cisco IoT Field Network Director could allow an unauthenticated remote attacker to cause a DoS condition on an affected drone. The vulnerability is due to insufficient inspection of incoming CoAP traffic. An attacker could exploit this vulnerability by sending a malformed CoAP packet to an affected drone. A successful exploit could allow an attacker to force the CoAP server to stop, interrupting communication with drone.

### 2.11 Vulnerabilities in the XMPP protocol

Drones use a client-side drone visual measurement tool [1]. The camera recording module provides the key functionality, the task of which is to transfer the data that has been recorded to the XMPP server and database.

The screen shows a camera image with a stop button in the lower left corner, a start button in the lower right corner, and a crosshair in the center of the screen.

The crosshair also allows the user to take a photo and save it to external memory.

The camera recording module is the main user interface of the program; recording data after selecting the record button on the camera screen.

The recorded step and direction information of the user is transmitted to a remote XMPP server in real time while the application is recording. Three buttons of the module trigger a separate action. The record button calls several functions that update sensor data, create a progress bar, and trigger an XMPP message sender. During recording, the floating-point sensor data is updated and transferred to the XMPP server in the best possible way. A data recording session lasts six seconds, resulting in approximately 57-59 sensor read packets being sent to the XMPP server. After the recording session ends, the data recording view can be used to continue offline tracking until the user explicitly selects the stop button. But the XMPP protocol has vulnerabilities shown in Fig. 9, which can lead to successful attacks.

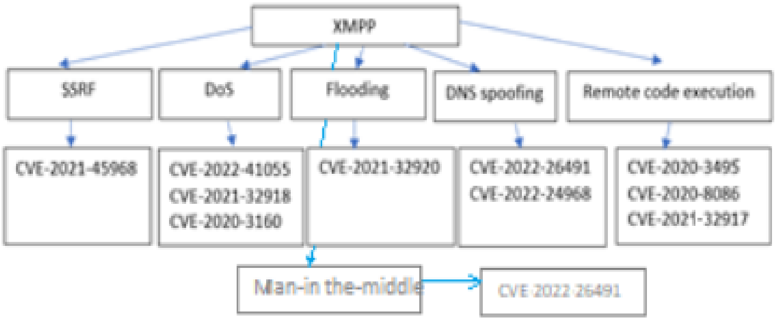


**Fig. 9.** Vulnerabilities in the protocol XMPP

### 2.12 Vulnerabilities in processors

The processors used in drones can also contain vulnerabilities. Potential security vulnerability CVE-2022-25899 (vulnerability with severity 9.9) [42] in Intel®-supported Open AMT Cloud Toolkit could allow an unauthenticated user to potentially enable privilege escalation via drone control access. There are also 2 of the most serious vulnerabilities that attackers can use to launch a successful cyber-attack. Meltdown (CVE-2017-5754), [43] allows a privileged attacker to read the entire memory of an attacked system via specially crafted executable code. An attacker must: gain physical access to the drone as an administrator, execute a specific program on the drone, read the protected data and send it back to the attacker. Specter [version 1: CVE-2017-5753, [44], version 2: CVE-2017-5715, [45] allows an attacker to read the memory of other processes using specially crafted executable code or dynamic code.

### 2.13 Vulnerabilities in the protocol SFTP (Secure File Transfer Protocol)

The drone can use the SFTP protocol to transfer data. SFTP protocol vulnerability CVE-2022-22899 [42] Core FTP / SFTP Server v2 Build 725 has been discovered to allow unauthenticated attackers to cause a denial of service (DoS) via a crafted packet via the SSH service.

### 2.14 Vulnerabilities in the protocol UART (Universal Asynchronous Transmitter)

CVE-2022-29402 - insecure protections in UART console, vulnerability allows attackers to connect to the UART port via a serial connection and execute commands as the root user without authentication [46].

### 2.15 Vulnerabilities in the protocol SPI

CVE-2021-26317 – verification of the protocol in SMM is failed, and may allow an attacker to control the protocol and modify SPI (Serial Peripheral Interface) flash resulting in a potential arbitrary code execution [47].

### 2.16 Vulnerabilities in the Protocol Controller Area Network (CAN)

CVE-2023-2166 was found in CAN protocol, which may not be initialized in the receive path of CAN frames. A local user could use this flaw to crash the system or potentially cause a DoS. Successful exploitation of the vulnerability on the drone may allow an attacker with physical access and extensive knowledge of CAN to reverse engineer network traffic to perform a DoS-attack disrupting the availability of arbitrary functions of the targeted device [48].

## 3 Systematization of Drone’s Vulnerabilities by Severities and Cyber-attacks

There are some organizations that collect vulnerability information, process it, and provide a severity score according to the Common Vulnerability Scoring System (CVSS), an open system for communicating the characteristics and severity of SW vulnerabilities. Tables 1-11 and Figures 10-16 provide comparative tables listing vulnerabilities in various communication protocols and possible attacks against them, along with the severity of successful attacks on these vulnerabilities. The "other database" column means that information about vulnerabilities can be presented in such databases as SUSE, Red Hat, Greenbone, Talos, Open Source Vulnerability Database (OSVDB), Common Vulnerability Enumeration (CWE) i The Open Web Application Security Project (OWASP) and others.

**Table 1.** DoS-attacks

| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| MQTT | CVE-2022-0671 | 9.1 | 6.4 | 9.1 |
| | CVE-2021-41039 | 7.5 | 5.0 | 7.5 |
| | CVE-2021-34431 | 6.5 | 5.0 | 6.5 |
| | CVE-2021-34432 | 7.5 | 5.0 | 7.5 |
| XMPP | CVE-2022-41055 | 7.5 | 5.0 | 7.5 |
| | CVE-2021-32918 | 7.5 | 5.0 | 7.5 |
| | CVE-2020-31060 | 5.3 | 5.0 | 5.3 |
| VPN | CVE-2022-25165 | 7.0 | 6.9 | 7.0 |
| | CVE-2022-20795 | 7.5 | 5.1 | 5.0 |
| | CVE-2022-20758 | 6.8 | 7.1 | 7.4 |
| | CVE-2022-25745 | 9.8 | 5.5 | 7.6 |
| | CVE-2022-20737 | 7.1 | 7.1 | 7.1 |
| | CVE-2022-20715 | 7.5 | 7.8 | 8.6 |
| | CVE-2022-1703 | 8.8 | 9.0 | 8.8 |
| SNMP | CVE-2022-26380 | 7.5 | 7.0 | 7.5 |
| | CVE-2022-22510 | 7.5 | 5.0 | 7.5 |
| | CVE-2022-22177 | 7.5 | 5.0 | 7.5 |
| | CVE-2022-20684 | 6.5 | 6.1 | 7.4 |
| | CVE-2022-20675 | 5.3 | 5.0 | 5.3 |
| NTP | CVE-2021-0227 | 7.5 | 4.0 | 7.5 |
| | CVE-2020-15025 | 4.9 | 4.0 | 4.4 |
| | CVE-2020-13817 | 7.4 | 5.8 | 5.9 |
| SSH | CVE-2022-22275 | 7.5 | 5.0 | 7.5 |
| | CVE-2022-22278 | 7.5 | 5.0 | 7.5 |
| | CVE-2022-24666 | 7.5 | 5.0 | 7.5 |
| | CVE-2022-24667 | 7.5 | 5.0 | 7.5 |
| | CVE-2022-24668 | 7.5 | 5.0 | 7.5 |
| | CVE-2022-0618 | 7.5 | 7.8 | 7.5 |
| | CVE-2022-24321 | 7.5 | 5.0 | 7.5 |
| | CVE-2022-22724 | 7.5 | 5.0 | 7.5 |
| | CVE-2022-23159 | 6.5 | 4.0 | 4.8 |
| | CVE-2022-22899 | 8.8 | 2.6 | - |
| | CVE-2022-20692 | 6.5 | 6.8 | 7.7 |

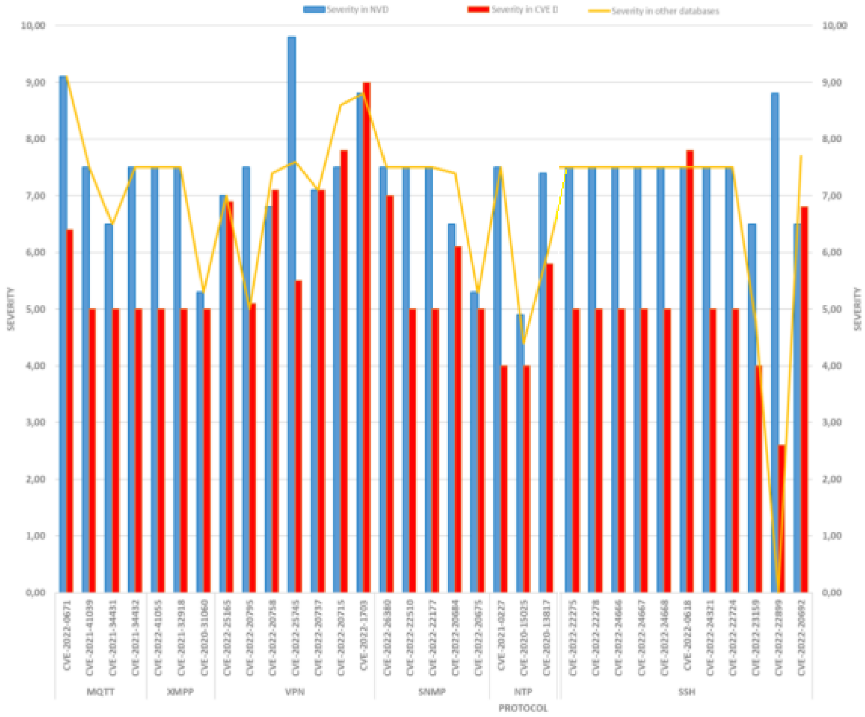


**Fig. 10.** Graphical dependence of the severity of the vulnerability on the types of vulnerability in the impact protocols DoS-attacks

**Table 2.** XSS-attacks

| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| VPN | CVE-2022-0734 | 6.1 | 4.3 | 5.8 |
| SSH | CVE-2022-21238 | 7.5 | 5.1 | 5.0 |
| | CVE-2022-26085 | 8.8 | 6.5 | 9.1 |
| | CVE-2022-23110 | 4.8 | 3.5 | - |
| NTP | CVE-2020-25498 | 4.8 | 3.5 | 4.8 |
| | CVE-2020-35262 | 6.1 | - | - |

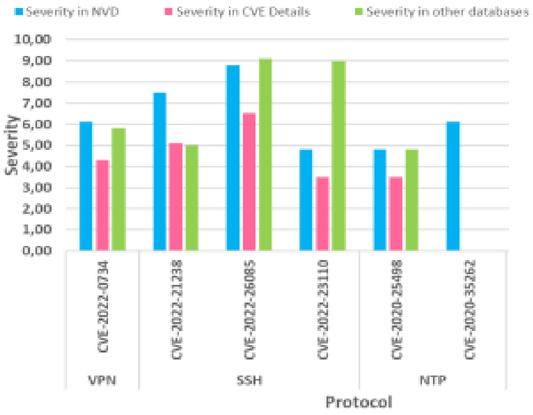


**Fig. 11.** Graphical dependences of the severity of vulnerabilities on the types of vulnerabilities in protocols when exposed XSS-attacks

**Table 3.** SSRF-attacks

| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| XMPP | CVE-2021-45968 | 7.5 | 5.0 | 7.5 |
| MQTT | CVE-2022-0671 | 9.1 | 6.4 | 6.4 |

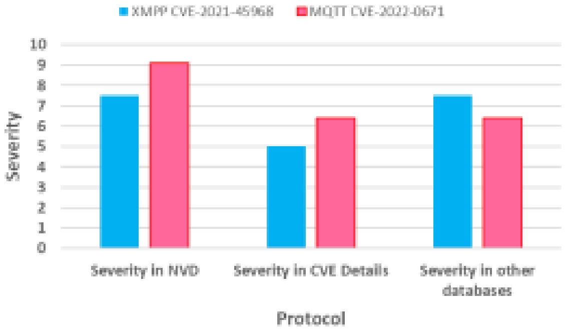


**Fig. 12.** Graphical dependences of the severity of vulnerabilities on the types of vulnerabilities in protocols and different databases under the influence of SSRF-attacks

**Table 4.** Flooding-attacks

| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| XMPP | CVE-2021-32920 | 7.5 | 7.8 | 7.5 |

**Table 5.** DNS-spoofing-attacks

| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| XMPP | CVE-2022-26491 | 5.9 | 6.4 | 5.9 |
|  | CVE-2022-24968 | 5.9 | 8.1 | 5.9 |

**Table 6.** Man-in-the-Middle-attacks

| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| VPN | CVE-2022-20742 | 7.4 | 5.8 | 7.4 |
| SNMP | CVE-2022-22156 | 7.4 | 5.8 | 6.5 |
| XMPP | CVE-2022-26491 | 5.9 | 6.4 | 5.9 |
| MQTT | CVE-2022-44549 | 7.4 | 5.8 | 7.4 |
|  | CVE-2022-41034 | 8.1 | 6.8 | 8.1 |
|  | CVE-2022-41033 | 8.1 | 6.8 | 8.1 |

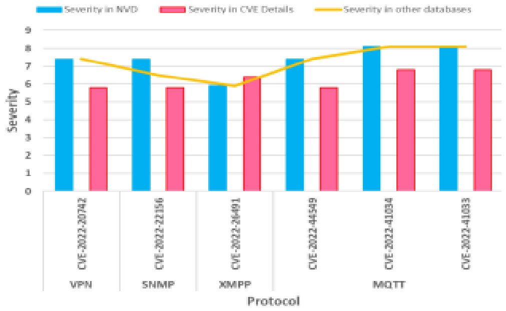


**Fig. 13.** Graphical dependences of the severity of vulnerabilities on the types of vulnerabilities in protocols in case of exposure to attacks Man-in-the-Middle

**Table 7.** Brute-force-attacks

| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| NTP | CVE-2022-22212 | - | 7.5 | 7.5 |

**Table 8.** Attacks to steal confidential information

| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| SNMP | CVE-2022-22277 | 5.3 | 5.0 | 5.3 |
|  | CVE-2022-22276 | 5.3 | 5.0 | 5.3 |

**Table 9.** SQL and others attacks of code injection

| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| VPN | CVE-2022-29383 | 9.8 | 7.5 | 9.8 |

**Table 10.** CSRF-attacks

| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| SSH | CVE-2022-27210 | 6.5 | 4.3 | 6.5 |
| | CVE-2022-30958 | 8.8 | 6.8 | 8.8 |
| | CVE-2022-25198 | 8.8 | 6.8 | 8.8 |
| | CVE-2022-23111 | 4.3 | 4.3 | 4.3 |

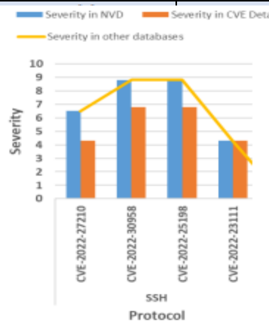


**Fig. 14.** Graphical dependences of criticality of vulnerabilities on types of vulnerabilities in protocols leading to CSRF-attacks

**Table 11.** Argument injection-attacks and OS commands

| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| VPN | CVE-2022-30525 | 9.8 | 10.0 | 9.8 |
| | CVE-2022-26532 | 7.8 | 7.3 | 7.8 |
| | CVE-2022-25165 | 7.0 | 6.9 | 6.9 |
| NTP | CVE-2022-27000 | 9.8 | 10 | 9.8 |
| | CVE-2020-26991 | 9.8 | 7.5 | 6.6 |
| | CVE-2020-9026 | 8.1 | 10.0 | 7.7 |
| | CVE-2020-9027 | 5.4 | 10.0 | 8.1 |
| | CVE-2022-7357 (1022) | 5.4 | 3.5 | 8.1 |
| | CVE-2022-9020 | 6.5 | 7.5 | 5.9 |
| | CVE-2022-10214 | 5.9 | 9.0 | 6.4 |
| | CVE-2022-30166 | 8.1 | 4.6 | 7.7 |

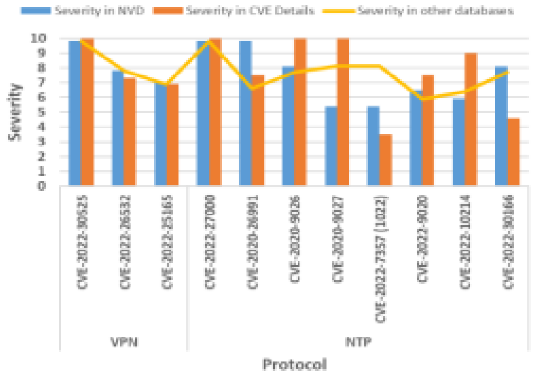
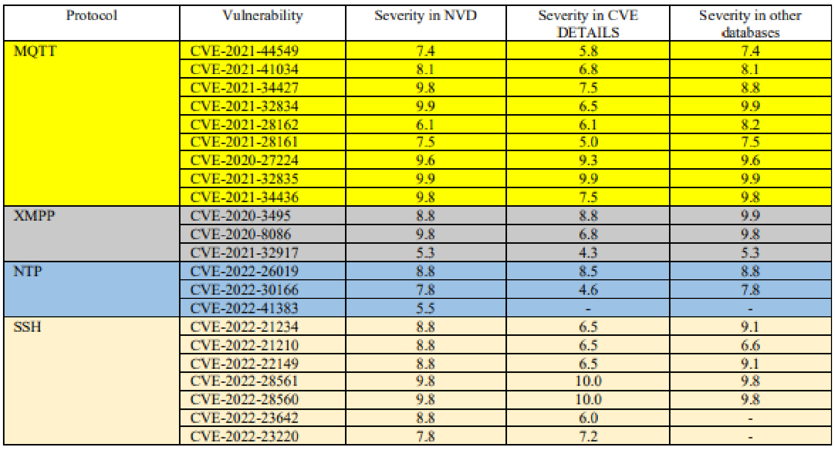


**Fig. 15.** Graphical dependences of the severity of vulnerabilities on the types of vulnerabilities in protocols, if the attacks of the injection of arguments and OS commands are affected

**Table 12.** Remote code-attacks and command execution



| Protocol | Vulnerability | Severity in NVD | Severity in CVE DETAILS | Severity in other databases |
|---|---|---|---|---|
| MQTT | CVE-2021-44549 | 7.4 | 5.8 | 7.4 |
| | CVE-2021-41034 | 8.1 | 6.8 | 8.1 |
| | CVE-2021-34427 | 9.8 | 7.5 | 8.8 |
| | CVE-2021-32834 | 9.9 | 6.5 | 9.9 |
| | CVE-2021-28162 | 6.1 | 6.1 | 8.2 |
| | CVE-2021-28161 | 7.5 | 5.0 | 7.5 |
| | CVE-2020-27224 | 9.6 | 9.3 | 9.6 |
| | CVE-2021-32835 | 9.9 | 9.9 | 9.9 |
| | CVE-2021-34436 | 9.8 | 7.5 | 9.8 |
| XMPP | CVE-2020-3495 | 8.8 | 8.8 | 9.9 |
| | CVE-2020-8086 | 9.8 | 6.8 | 9.8 |
| | CVE-2021-32917 | 5.3 | 4.3 | 5.3 |
| NTP | CVE-2022-26019 | 8.8 | 8.5 | 8.8 |
| | CVE-2022-30166 | 7.8 | 4.6 | 7.8 |
| | CVE-2022-41383 | 5.5 | - | - |
| SSH | CVE-2022-21234 | 8.8 | 6.5 | 9.1 |
| | CVE-2022-21210 | 8.8 | 6.5 | 6.6 |
| | CVE-2022-22149 | 8.8 | 6.5 | 9.1 |
| | CVE-2022-28561 | 9.8 | 10.0 | 9.8 |
| | CVE-2022-28560 | 9.8 | 10.0 | 9.8 |
| | CVE-2022-23642 | 8.8 | 6.0 | - |
| | CVE-2022-23220 | 7.8 | 7.2 | - |

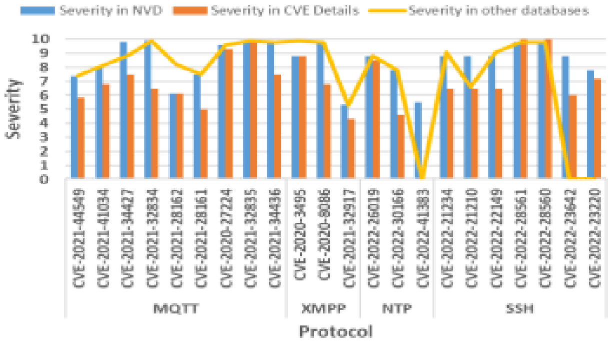


**Fig. 16.** Graphical dependences of the severity of vulnerabilities on the types of vulnerabilities in protocols in the case of an attack on remote code and command execution

Graphical dependencies show how the severity values of the same vulnerability differ, but in different vulnerability databases.

## Conclusions

In this paper was realized the system analysis of drone's subsystems, and was made the analysis and the systematization of vulnerabilities in its subsystems.

Were analyzed cyber-attacks, which can impact to these vulnerabilities.

The drone may be connected to the global Internet access network and may also be affected by attacks used in conventional computer networks. Cyber-attacks on a drone can be carried out when connected to its interfaces, using wireless Internet access technologies through a 4G/5G router or modem.

The each considered vulnerability is a hole in cybersecurity.

From the moment a vulnerability is discovered to the moment a patch is installed for it, the minimum time should pass, since during this period of time attackers can successfully attack vulnerabilities known to them. Therefore, it is very important to update SW versions and fix vulnerabilities in a timely manner.

Drone uses VPN, but the number of VPN vulnerabilities has increased recently. Therefore, it is necessary to take measures for their additional cyber protection.

The conducted analysis showed that the vulnerabilities of drones are in the used general information transfer protocols, in HW and SW. The most of attacks on modern drones, which use vulnerabilities, are various types of DoS-attacks, Man-in-the-Middle-attacks and remote code execution attacks.

The analysis and the systematization of vulnerabilities and cyber-attacks on drones will allow drone manufacturers and users to propose new measures and update recommendations for ensuring cybersecurity for all drone components.

Further research will be aimed at developing a method for prioritizing drone vulnerabilities a method of evaluating and ensuring their dependability, which will increase the reliability and cybersecurity of drones.

## References

1. Autonomian. UAV Data Transmissionand Protocols. https://robolabor.ee/img/cms/projektid/UAV%20Data%20Transmission%20and%20 Communication%20Protocols.pdf. 92 p., last accessed 2023/04/04.
2. Yanmaz, E., Yahyanejad, S., Rinner, B., Hellwagner, H., Bettstetter, Ch.: Drone Networks: Communications, Coordination, and Sensing. Ad Hoc Networks. (2017). 68. 10.1016/j.adhoc.2017.09.001.
3. Pleban, J., Band, R., Creutzburg, R.: Hacking and securing the AR.Drone 2.0 quadcopter - Investigations for improving the security of a toy. (2014). 10.1117/12.2044868.
4. Menoret, S., Auburg, T., Nousi, V., Pitas Aristotle, I.: Drone communications. European Union’s Horizon 2020 research and innovation programmed under grant agreement. No 731667 (MULTIDRONE).
5. Sawalmeh, A., Othman, N.: An Overview of Collision Avoidance Approaches and Network Architecture of Unmanned Aerial Vehicles (UAVs). International Journal of Engineering & Technology. 7. 10.14419/IJET.v7i4.35.27395. (2018).
6. Aranzazu Suescun, C., Cardei, M.: Unmanned Aerial Vehicle Networking Protocols. (2021). 10.18687/LACCEI2016.1.S.078.
7. Aldeen, S., Yousra, Abdulhadi, H.: Data communication for drone-enabled internet of things. Indonesian Journal of Electrical Engineering and Computer Science. 22. 1216. (2021). 10.11591/IJEECS.v22.i2.pp1216-1222.
8. Kwon, Y.M.; Yu, J.; Cho, B.M.; Eun, Y.; Park, K.J.: Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles. IEEE Access 6, 43203–43212. (2018).
9. Khan, N., Zaman, N., Brohi, S., Almazroi, A.: A Secure Communication Protocol for Unmanned Aerial Vehicles. Computers, Materials and Continua. 70. pp. 601-618. (2021). 10.32604/cmc.2022.019419.
10. Aerosmart. UAV systems and solutions. Use-case. Drone Detection System. (2022). https://www.aerosmart.ae/drone-detection-system/ last accessed 2023/04/05.

11. Kaspersky. Endpoint Security for Linux. For workstations and servers. https://www.kaspersky.com/small-to-medium-business-security/endpoint-linux, last accessed 2023/04/05.
12. Lee, M., Choi, G., Park, J. and S. Cho: Study of Analyzing and Mitigating Vulnerabilities in uC/OS Real-Time Operating System, 2018 Tenth International CONFERENCE on Ubiquitous and Future Networks (ICUFN). pp. 834-836. (2018). doi: 10.1109/ICUFN.2018.8436965.
13. Belding, G.: Malware spotlight: EvilGnome. (2020). https://resources.infosecinstitute.com/topic/malware-spotlight-evilgnome/, last accessed 2023/04/10.
14. National vulnerability database. CVE-2020-14314, https://nvd.nist.gov/vuln/detail/CVE-2020-14314, last accessed 2023/04/05.
15. National vulnerability database. CVE-2020-16119, https://nvd.nist.gov/vuln/detail/CVE-2020-16119, last accessed 2023/04/10.
16. Linux RedHat, https://access.redhat.com/security/cve/cve-2020-16119, last accessed 2023/04/10.
17. National vulnerability database. CVE-2020-16120, https://nvd.nist.gov/vuln/detail/CVE-2020-16120 last accessed 2023/04/10.
18. National vulnerability database. CVE-2020-14385. [Online access]: https://nvd.nist.gov/vuln/detail/CVE-2020-14385.
19. National vulnerability database. CVE-2020-20285, https://nvd.nist.gov/vuln/detail/CVE-2020-20285, last accessed 2023/04/10.
20. National vulnerability database. CVE-2020-25641, https://nvd.nist.gov/vuln/detail/CVE-2020-25641, last accessed 2023/04/10.
21. National vulnerability database. CVE-2022-23222, https://nvd.nist.gov/vuln/detail/CVE-2020-23222 last accessed 2023/04/10.
22. RedHat, https://bugzilla.redhat.com/show_bug.cgi?id=2119048, last accessed 2023/04/10.
23. RedHat, https://bugzilla.redhat.com/show_bug.cgi?id=2188396, last accessed 2023/04/10.
24. MITRE. CVE-2021-1378, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1378, last accessed 2023/04/10.
25. National vulnerability database. CVE-2021-1378, https://nvd.nist.gov/vuln/detail/CVE-2021-1378, last accessed 2023/04/10.
26. National vulnerability database. CVE-2021-1592, https://nvd.nist.gov/vuln/detail/CVE-2021-1592, last accessed 2023/04/10.
27. National vulnerability database. CVE-2020-15025, https://nvd.nist.gov/vuln/detail/CVE-2020-15025, last accessed 2023/04/10.
28. National vulnerability database. CVE-2020-13817, https://nvd.nist.gov/vuln/detail/CVE-2020-13817, last accessed 2023/04/10.
29. National vulnerability database. CVE-2020-11868, https://nvd.nist.gov/vuln/detail/CVE-2020-11868, last accessed 2023/04/10.
30. National vulnerability database. CVE-2022-27000, https://nvd.nist.gov/vuln/detail/CVE-2022-27000, last accessed 2023/04/10.
31. National vulnerability database. CVE-2022-26019, https://nvd.nist.gov/vuln/detail/CVE-2022-26019, last accessed 2023/04/10.
32. National vulnerability database. CVE-2018-0280, https://nvd.nist.gov/vuln/detail/CVE-2018-0280, last accessed 2023/04/10.
33. National vulnerability database. CVE-2022-21722, https://nvd.nist.gov/vuln/detail/CVE-2022-21722, last accessed 2023/04/10.

34. Burleson-Davis, J.: 7 Common VPN Security Risks: The Not-So-Good, The Bad, and the Ugly. April 14, 2021. //https://www.securelink.com/blog/vpnproblems/#:~:text=VPNs%20are%20insecure%20because%20they,network%20can%20be%20brought%20down, last accessed 2023/04/10.
35. Aljehani, Maher & Inoue, Masahiro: Communication and Autonomous Control of Multi-UAV System in Disaster Response Tasks. (2017). 10.1007/978-3-319-59394-4_12.
36. Rametta, C., Beritelli, F., Avanzato R. and Russo M.: A Smart VPN Bonding Technique for Drone Communication Applications, 2019 15th International CONFERENCE on Distributed Computing in Sensor Systems (DCOSS), (2019). pp. 612-618, DOI: 10.1109/DCOSS.2019.00112.
37. National vulnerability database. CVE-2022-22510, https://nvd.nist.gov/vuln/detail/CVE-2022-22510, last accessed 2023/04/15.
38. National vulnerability database. CVE-2022-22510, https://nvd.nist.gov/vuln/detail/CVE-2022-22510, last accessed 2023/04/15.
39. Husnain, Muhammad & Hayat, Khizar & Cambiaso, Enrico & Fayyaz, Ubaid & Mongelli, Maurizio & Akram, Habiba & Abbas, Syed & Shah, Ghalib. Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System. Sensors (2022). 22. 567. 10.3390/s22020567.
40. National vulnerability database. CVE-2022-0673, https://nvd.nist.gov/vuln/detail/CVE-2022-0673, last accessed 2023/04/21.
41. National vulnerability database. CVE-2020-3162, https://nvd.nist.gov/vuln/detail/CVE-2020-3162, last accessed 2023/04/21.
42. National vulnerability database. CVE-2022-22899, https://nvd.nist.gov/vuln/detail/CVE-2022-22899, last accessed 2023/04/21.
43. National vulnerability database. CVE-2017-5754, https://nvd.nist.gov/vuln/detail/CVE-2017-5754, last accessed 2023/04/21.
44. National vulnerability database. CVE-2017-5753, https://nvd.nist.gov/vuln/detail/CVE-2017-5753, last accessed 2023/04/21.
45. National vulnerability database. CVE-2017-5753, https://nvd.nist.gov/vuln/detail/CVE-2017-5753, last accessed 2023/04/21.
46. National vulnerability database. CVE-2022-29402, https://nvd.nist.gov/vuln/detail/cve-2022-29402, last accessed 2023/05/05.
47. National vulnerability database. CVE-2021-26317, https://nvd.nist.gov/vuln/detail/CVE-2021-26317, last accessed 2023/04/21.
48. National vulnerability database. CVE-2023-2166, https://nvd.nist.gov/vuln/detail/CVE-2022-2166, last accessed 2023/04/21.