Vulnerability Identification of Local IoT Devices via Wardriving

Authors

Yingli Duan - s222462

May 31, 2023

Contents

1 Introduction

With the proliferation of Internet of Things (IoT) devices, our lives have become increasingly intertwined with these interconnected systems, spanning various domains such as healthcare, smart mobile devices, and transportation. As IoT devices transmit sensitive information and facilitate seamless communication between devices, they have become prime targets for malicious actors.

Among the myriad wireless technologies employed in the IoT landscape, WiFi and Bluetooth stand out as the most widely utilized. Consequently, they have become prime targets for security breaches. For instance, on January 23, 2023, a significant server-side request forgery (SSRF) vulnerability was discovered in Lexmark devices, earning a high base score of 9.0 according to the Common Vulnerability Scoring System (CVSS) v3. This vulnerability impacted a substantial number of devices[1].

In order to raise awareness regarding IoT security, this report sheds light on the vulnerabilities prevalent in WiFi and Bluetooth technologies. The analysis presented herein is based on data acquired through Wardriving, a method of collecting wireless network data.

The structure of this report is as follows:

- Analysis Methodology: This section outlines the approach adopted for data collection and subsequent statistical analysis.
- Bluetooth Vulnerabilities: This section presents the analysis results pertaining to Bluetooth vulnerabilities. Devices are categorized into seven major device types, and the vulnerabilities are showcased in relation to the respective vendors.
- WiFi Vulnerabilities: Given the challenge of differentiating device types within WiFi networks, the statistical results in this section are organized solely based on vendors.
- Discussion: This section offers an objective evaluation of the findings presented in this report and provides valuable insights for future improvements and advancements.

[1] `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23560`

2 Methodology

Divided into two parts, our research comprises 5 phases. The first part is information collection, which is taken in the first two steps: collecting and extracting data. After extracting keywords from the first step, vulnerabilities will be collected by using these keywords in the second step and then analyzed.

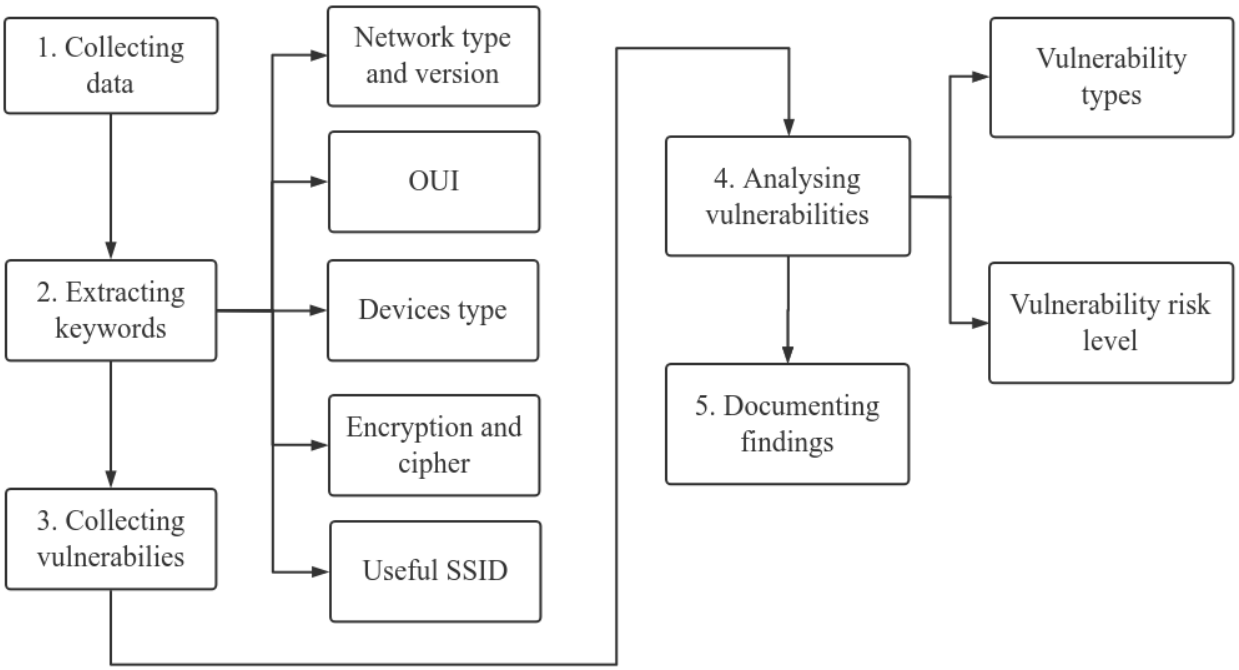

Figure 1: Methodology for IoT network vulnerability analysis

Step 1. We walk around the city with phones with WiGLE installed. After collecting more than 1 million, we start to enrich the data information by using some public access databases. By using the IEEE public registration authority list[2], the vendor name of each device can be identified through the corresponding OUI (Organizationally Unique Identifier). Figure 2 illustrates the process. Finally, as the preparation for the next step, we extract those keywords needed for collection vulnerabilities and process statistics of them.

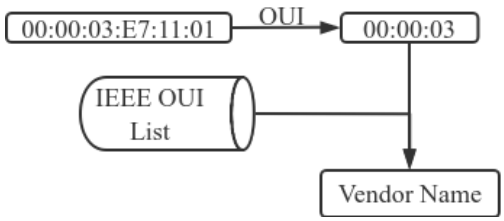

Figure 2: Extract vendor name of devices with MAC 00:00:03:E7:11:01

[2] https://standards.ieee.org/products-programs/regauth/

```
[{'id': 'CVE-2023-31199', 'summary': 'Improper access control in the
Intel(R) Solid State Drive Toolbox(TM) before version 3.4.5 may allow a
privileged user to potentially enable escalation of privilege via local
access.', 'created_at': '2023-05-12T15:15:00Z', 'updated_at':
'2023-05-24T15:46:00Z'},
{'id': 'CVE-2023-31197', 'summary': 'Uncontrolled search path in the
Intel(R) Trace Analyzer and Collector before version 2020 update 3 may allow
an authenticated user to potentially enable escalation of privilege via
local access.', 'created_at': '2023-05-12T15:15:00Z', 'updated_at':
'2023-05-24T15:42:00Z'},
```


Figure 3: Parts of results of vulnerabilities of Intel by invoking OpenCVE API

For Bluetooth devices, network version, vendor name, and device types are used as keywords. As for device types, they can be found in the *capabilities* field directly. What's more, we can also find hints about device types from *SSID*. For example, the devices with SSID Beoplay HX are headphones and the devices with SSID contained [TV] are TV, which are Display/Speaker types.

Considering Wi-Fi devices, WiGLE provides us with OUI, devices encryption protocols and cipher information.

Step 2. In this part, vulnerabilities of IoT devices are collected by using public APIs: OpenCVE[3] and NVD vulnerabilities APIs[4].

For the precision of results, vendor names cannot be used as keywords in API directly. For example, we want to search for the vulnerabilities of LG products. If we search *LG* directly as keywords, all the vulnerabilities, whose descriptions contain the words *algorithm* will all be written into JSON data and send as results, because *LG* is contained in words *al**lg**orithm*

The API invoking method is shown below:

- **Vendor name as keywords:** The vendor names should be extracted first. For example, the company *Samsung Electronics Co.,Ltd* should be cleaned as *samsung*, which is the name displayed in CPE[5]. Afterwards, invoking OpenCVE APIs to obtain all the CVE ids belonging to the vendor. Figure 3 shows part of the result of vendor Intel. Finally, NVD API is invoked to collect the details of the CVEs. Figure 4 is the result of CVE-2023-31199. In this picture, we can obtain the vulnerability description in key *descriptions*, the vulnerability risk level is in key *metrics* → *baseSeverity*, and the weakness type is in key *weaknesses* → *value*. Thus, according to the results, the risk level of CVE-2023-31199 is 7.8(high), and the risk type is CWE-427. We will explain the meaning of CWE(Common Weakness Enumeration) later.
- **Others as keywords** And other keywords can be searched by NVD API directly.

Vulnerabilities analysis comes after loading all the vulnerabilities into the database. In this step, we only analyze vulnerabilities from 2021. Weakness types and risk levels are our core points. In NVD, each type of weakness is represented by a unique CWE id. Picture 5

[3] https://docs.opencve.io/
[4] https://nvd.nist.gov/developers/vulnerabilities#
[5] https://nvd.nist.gov/products/cpe

```
'vulnerabilities': [{'cve': {'id': 'CVE-2023-31197', 'sourceIdentifier':
'secure@intel.com', 'published': '2023-05-12T15:15:09.470', 'lastModified':
'2023-05-24T15:42:14.870', 'vulnStatus': 'Analyzed',
'descriptions': [{'lang': 'en', 'value': 'Uncontrolled search path in the
Intel(R) Trace Analyzer and Collector before version 2020 update 3 may allow
an authenticated user to potentially enable escalation of privilege via
local access.'}],
'metrics': {'cvssMetricV31': [{'source': 'nvd@nist.gov', 'type': 'Primary',
'cvssData': {'version': '3.1', 'vectorString':
'CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H', 'attackVector': 'LOCAL',
'attackComplexity': 'LOW', 'privilegesRequired': 'LOW', 'userInteraction':
'NONE', 'scope': 'UNCHANGED', 'confidentialityImpact': 'HIGH',
'integrityImpact': 'HIGH', 'availabilityImpact': 'HIGH', 'baseScore': 7.8,
'baseSeverity': 'HIGH'}, 'exploitabilityScore': 1.8, 'impactScore': 5.9},
{'source': 'secure@intel.com', 'type': 'Secondary', 'cvssData': {'version':
'3.1', 'vectorString': 'CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H',
'attackVector': 'LOCAL', 'attackComplexity': 'HIGH', 'privilegesRequired':
'LOW', 'userInteraction': 'REQUIRED', 'scope': 'UNCHANGED',
'confidentialityImpact': 'HIGH', 'integrityImpact': 'HIGH',
'availabilityImpact': 'HIGH', 'baseScore': 6.7, 'baseSeverity': 'MEDIUM'},
'exploitabilityScore': 0.8, 'impactScore': 5.9}]},
'weaknesses': [{'source': 'nvd@nist.gov', 'type': 'Primary', 'description':
[{'lang': 'en', 'value': 'CWE-427'}]}],
```


Figure 4: NVD API data of vulnerability CVE-2023-31197

demonstrates some examples of weakness types of CWE in NVD vulnerability search page[6]. Thus, according to the CWE mapping list shown in picture 5, the vulnerability we discussed above is a **Buffer Over-read** vulnerability. Risk levels are assessed by CVSS (Common Vulnerability Scoring System) version 3.

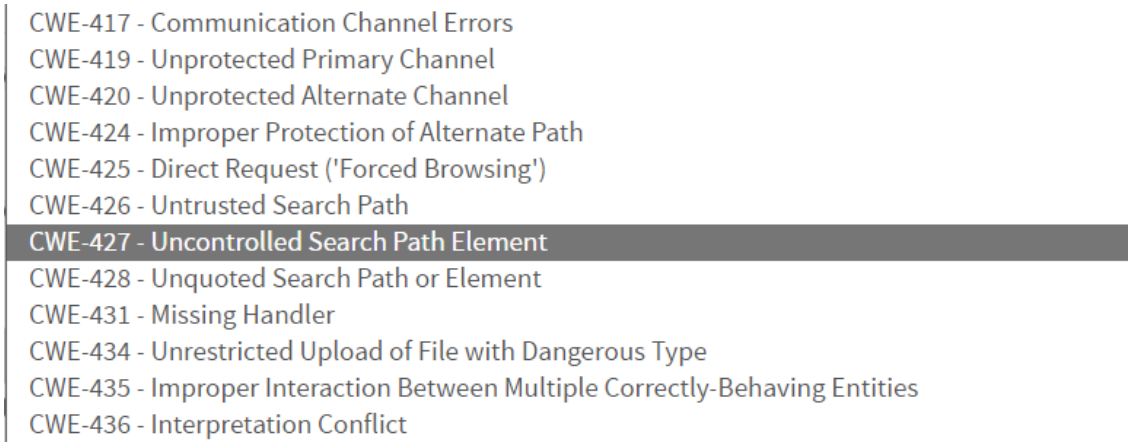

Figure 5: CWE list in NVD

Noticeably, as can be seen in picture 4, the *cvssMetricV31* is followed by a list value, which means one CVE can be assessed by many Metrics. Same with *weaknesses*, one CVE can fall into different value types. As a consequence, the total number of vulnerabilities via risk level and via types will be a little gap.

[6] `https://nvd.nist.gov/vuln/search`

3 Vulnerabilities of Bluetooth

In this section, we focus on the analysis of vulnerabilities present in Bluetooth devices. Building upon the methodology outlined in Step 12, specific keywords were employed to search for vulnerabilities. Subsequently, Subsection 3.1 presents an overview of the statistical analysis conducted on these keywords, along with the classification of devices into seven major classes. To further investigate the vulnerabilities inherent in Bluetooth devices, we proceed with an analysis of vulnerability types and risk levels for each device group in Sections 3.2 and 3.3 respectively.

3.1 Overview

bssid	ssid	equenc	capabilities	lasttime	lastlat	lastlon	type
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
cc:f9:57:...	6119604...	256	Computer;10	1678188432000	55.7829785021022	12.5176837295294	B
cc:f9:57:...	4EB7354...	256	Computer;10	1678223132000	55.7097131665796	12.4652312044054	B
cc:f9:57:...	02B82A...	256	Computer;10	1678265605000	55.7577580260113	12.5021339580417	B
cc:f9:57:...	095CE4...	256	Computer;10	1677766209428	55.7892416051329	12.5251036127355	E
cc:f9:57:...	B7CFC6...	256	Computer;10	1677595269716	55.7804664956448	12.5163779851333	E
cc:f9:57:...	791A3C...	256	Computer;10	1677791164000	55.7071838241724	12.4571798064114	E
cc:f9:57:...	391E11E...	256	Computer;10	1678175292000	55.7576748356223	12.5018525775522	E

Figure 6: Bluetooth data in WiGLE

A total of 835,453 Bluetooth access points were collected as part of the research. Figure 6 provides an illustration of the data obtained from the database, including MAC addresses, device types, and Bluetooth versions. The vendor name can be deduced from the MAC address.

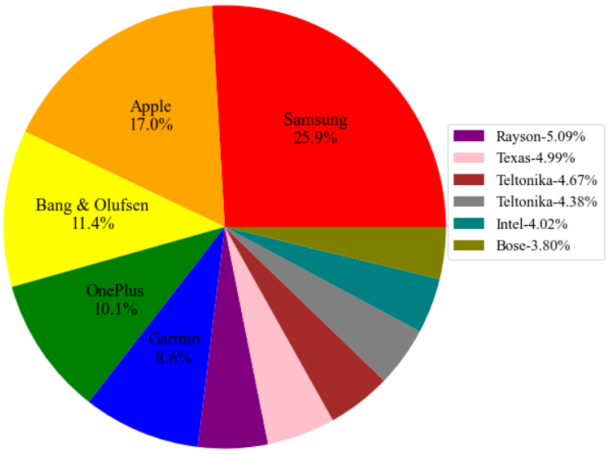

Figure 7: Top 7 Bluetooth Vendors from 2021

The Bluetooth market in 2021 comprises a minimum of 2405 vendors, each with a specific market share. Among them, the top 7 vendors with the highest usage of Bluetooth products are highlighted in Figure 7. Notably, Samsung and Apple dominate the market, holding a significant market share of 25.9

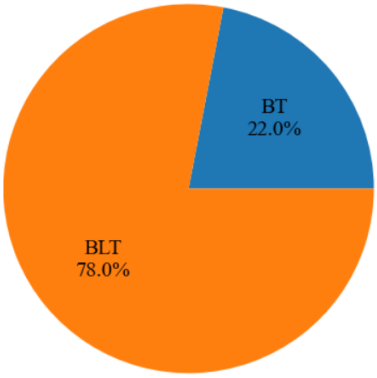

Figure 8: Bluetooth Versions from 2021

Regarding Bluetooth versions, the majority of the identified devices utilize Bluetooth Low Energy (BLE), accounting for 78.2% of the market, as depicted in Figure 8.

Table 1: Devices types of Bluetooth from 2021

Major classes	Minor classes	count	%	Major classes	Minor classes	count	%
	Uncatego-rized /Misc	822427	-1	Computer	PDA	71	0.17
Video/ Audio	Headphones	20434	49.60	Video/ Audio	A/V	35	0.08
Video/ Audio	Handsfree	4695	11.40	Computer	Palm	16	0.04
Phone	Smartphone	4574	11.10	Phone	Cordless Phone	13	0.03
Imaging	Display/ Speaker	4286	10.40	Video/ Audio	Monitor	11	0.03
Peripheral	Peripheral	3611	8.77	Health	Pulse	10	0.02
Health	Health	1309	3.18	Health	PulseOxy	9	0.02
Wearable	Watch	836	2.03	Health	Health Display	8	0.02
Phone	Phones	281	0.68	Wearable	Wearable	8	0.02
Computer	Computer	213	0.52	Computer	Computer Server	6	0.01

Continued on next page

Table 1 – continued from previous page

Major classes	Minor classes	count	%	Major classes	Minor classes	count	%
Video/ Audio	Settop	192	0.47	Wearable	Wearable	6	0.01
Computer	Desktop	189	0.46	Video/ Audio	VCR	6	0.01
Phone	Cellphone	187	0.45	Toy	Robot	5	0.01
Video/ Audio	CarAudio	102	0.25	Video/ Audio	Portable Audio	2	0.00
Video/ Audio	HiFi	79	0.19	Toy	Toy	2	0.00

For the subsequent vulnerability statistics, we map the minor device classes obtained from WiGLE directly to major categories [1]. Table 1 presents the detected devices belonging to seven major classes: Video/Audio, Phone, Peripheral, Health, Computer, Toy, and Wearable. The column labelled "%" excludes the amount of Uncategorized/Misc devices in the sum, with the percentage of Uncategorized/Misc set as -1.

More than half of the Bluetooth devices fall under the Video/Audio category, particularly the minor class "Headphones," which accounts for nearly 50% of all devices. Additionally, *Handsfree,Smartphone*, and *Display/Speaker* each constitute approximately 11% of the devices.

Consequently, we can utilize the vendor name, Bluetooth version, and device type as keywords to search for vulnerabilities in Bluetooth devices. The following two subsections provide a detailed analysis of the vulnerability statistics.

3.2 Types of Vulnerabilities

A total of 46 types of vulnerabilities have been identified in Bluetooth devices. In this subsection, we will provide an overview of the vulnerabilities across all detected devices and then delve into each group of devices individually.

Figure 9 presents the 22 most prevalent vulnerabilities. We have categorized these vulnerabilities decrease from left to right according to the total number of vulnerabilities. The heatmap depicting the distribution of Bluetooth vulnerabilities can be found in Appendix 7.1.

Among the top 22 vulnerabilities, the most common types include *Classic Buffer-Overflow*, *Out-of-bounds Write*, and *NULL Pointer Dereference*, all falling under the category of **Buffer Overflow**, with a total of 40 vulnerabilities. Besides, *Memory Buffer Bounds Violation*, *Heap-based Buffer Overflow* can also be regarded as buffer overflow. **Cross-site Scripting** is the second most one.

Some **Authentication and Authorization Issues** are prominent as well, like *Missing*

Authentication for Critical Function, *Incorrect Authorization* and *Improper Authorization*.

The vendors are listed in descending order from bottom to top based on the total number of vulnerabilities. Intel leads the way with 24 vulnerabilities among the top 22 most prevalent types. It is followed by Realtek (REALTEK SEMICONDUCTOR CORP.), NVIDIA, Bosch, and Lenovo.

Figure 9: Top 22 vulnerabilities of Bluetooth

Figure 10 presents the distribution of vulnerabilities in Bluetooth devices, while figures 11 to 15 provide a detailed breakdown of vulnerabilities for each major device class. In figures 11 to 15, the pie charts illustrate the distribution of vulnerabilities based on CWE categories and

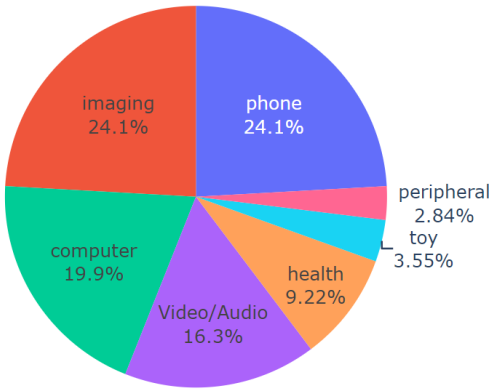

Figure 10: Vulnerabilities of 7 Categories Bluetooth Devices

the corresponding vendors, while the bar charts display the overall number of vulnerabilities for each class.

Notably, approximately 50% of the vulnerabilities are found in the Imaging and Phone classes, with each class accounting for 24.1%. And the proportion of Health, Toy and Peripheral class are below 10%. Further analysis and insights will be discussed in the subsequent part in order of the number of vulnerabilities.

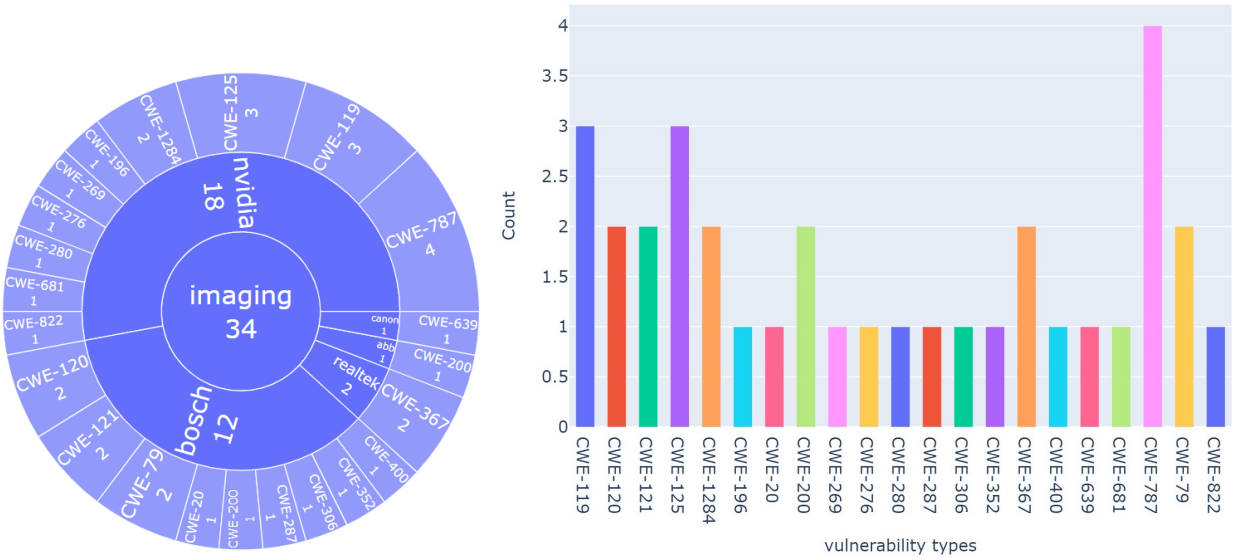

Figure 11: Vulnerabilities of Imaging class devices via types

For **Imagining** classes, NVIDIA[7] is responsible for 18 vulnerabilities, while Bosch[8] has 12 vulnerabilities associated with their products.

The main types of vulnerabilities identified in the Imaging devices, along with some examples of CVEs, are as follows:

[7] https://www.nvidia.com/en-us/
[8] https://www.boschsecurity.com/xc/en/

- CWE-787: Out-of-bounds Write.(NVIDIA).**CVE-2023-0191:** A vulnerability is found in the display driver, which causes many potentials threat like DoS, and information disclosure.
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer(NVIDIA) **CVE-2023-0188:** An out-of-bounds access vulnerability in the kernel mode layer handler can cause the DoS or data tempering.
- CWE-125: Out-of-bounds Read(NVIDIA).**CVE-2023-0188:** An unprivileged user can cause improper restriction of operations within the bounds of the memory buffer. the display driver

It is evident that buffer overflow is the primary concern in the Imaging class. In addition to the above weaknesses, other types of buffer overflow vulnerabilities include Stack-based Buffer Overflow (CWE-120) and Buffer Copy without Checking the Size of Input ('Classic Buffer Overflow') (CWE-121).

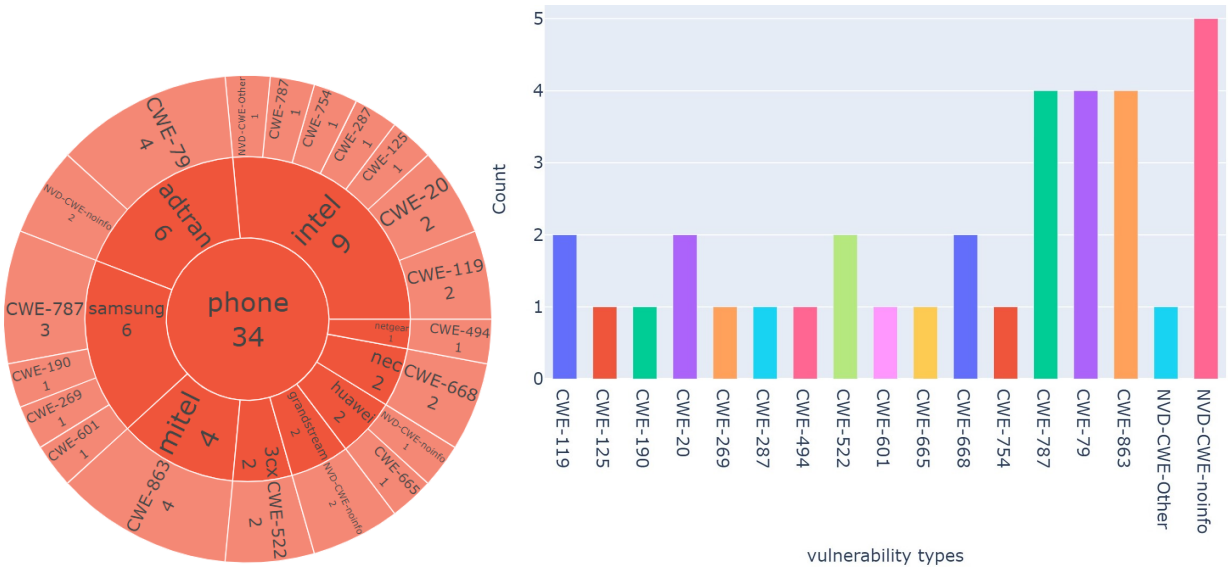

Figure 12: Vulnerabilities of Phone class devices via types

For **Phone** classes devices, the vulnerabilities primarily originate from Intel (8), Samsung (6), Adtran[9] (4), and Mitel[10] (4) in terms of vendor contributions. The main types of vulnerabilities identified are as follows:

- CWE-79: Cross-site Scripting.(Adtran Inc).**CVE-2021-25679:** The AdTran Personal Phone Manager software has an authenticated stored cross-site scripting (XSS) vulnerability, which affects versions 10.8.1 and below, and potentially later versions.
- CWE-863: Incorrect Authorization.(Mitel Networks Corporation). **CVE-2022-29854:** It allowed hackers, who have physical access to the phone, to obtain the root access, because of the insufficient access control. Being exploited, the system allowed an attacker access to sensitive information and code execution.

[9] https://www.adtran.com/
[10] https://www.mitel.com/

- CWE-787: Out-of-bounds Write.(SAMSUNG and Intel). **CVE-2023-21458:** The hacker can turn off Do not disturb mode because of improper privilege in the PhoneStatusBarPolicy in System UI.

In Phone class devices, buffer overflow and improper authentication are also significant concerns. CWE-119, CWE-125, and CWE-787 can be categorized as buffer overflow vulnerabilities, while CWE-269, CWE-287, CWE-522, and CWE-863 are related to authentication problems. Additionally, the presence of XSS vulnerability (CWE-79) is more prominent in the Phone class compared to the Imaging class.

Notably, one vulnerability (**CVE-2022-27639**) associated with Intel products falls into the NVD-CWE-Other category. It involves certain Intel(R) XMM(TM) 7560 Modem software versions, commonly used in smartphones, having a vulnerability related to incomplete cleanup. Exploiting this vulnerability, a privileged user could potentially escalate their privileges through adjacent access. Furthermore, **CVE-2022-48353** is an example of an NVD-CWE-noinfo vulnerability originating from Huawei[11]. It indicates that certain smartphones may experience configuration issues that can potentially be exploited. Successful exploitation of this vulnerability could result in the escalation of kernel privileges, leading to exceptions within system services.

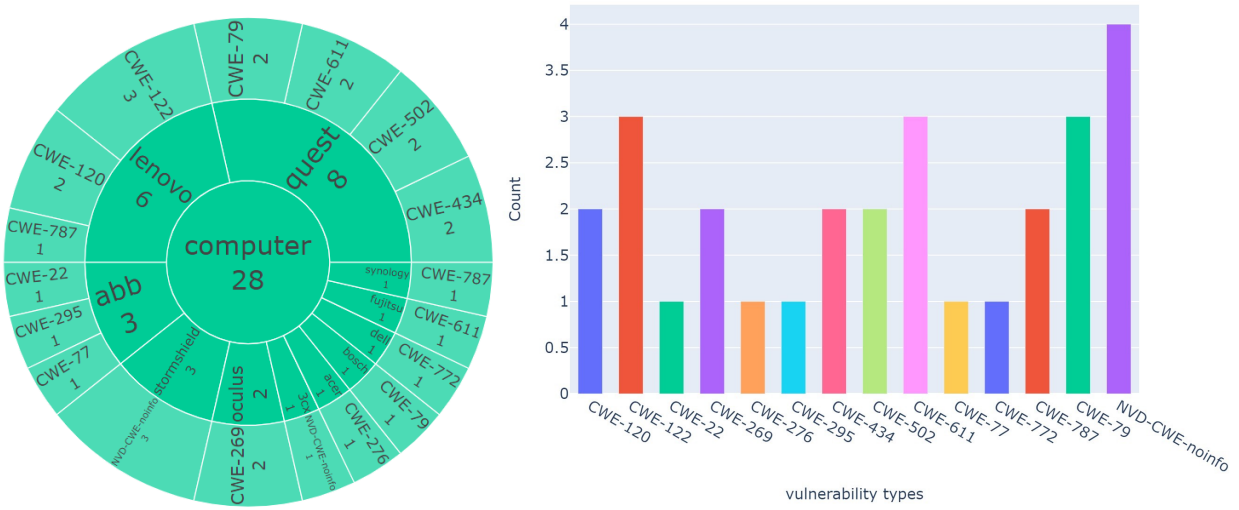

Figure 13: Vulnerabilities of Computer class devices via types

For **Computer** class devices, Quest[12], Lenovo[13] contribute more than half of vulnerabilities. the main types of vulnerabilities are:

- CWE-122: Heap-based Buffer Overflow. (Lenovo). **CVE-2022-1892:** An attacker with local privileges can execute arbitrary code because of a buffer overflow in Lenovo laptop products.

[11] https://consumer.huawei.com/en/
[12] https://www.quest.com/
[13] https://www.lenovo.com/dk/da/pc

- CWE-79: Cross-site Scripting. (Quest Software, Inc. and Robert Bosch Smart Home GmbH).**CVE-2021-23856:**The presence of a reflected XSS vulnerability on the web server allows attackers to potentially execute malicious scripts on a client's computer by tricking them into accessing a specially crafted URL.
- CWE-611:Improper Restriction of XML External Entity Reference. (Quest Software, Inc. and Fujitsu [14]).

Figure 14: Vulnerabilities of Video/Audio class devices via types

For **Video/Audio** class devices, Realtek[15] is responsible for 8 vulnerabilities, followed by Synology[16] with 4 vulnerabilities, and Sony with 3 vulnerabilities. Interestingly, within the Video/Audio class, 9 vulnerabilities are categorized as NVD-CWE-noinfo, which is twice the number of the second most vulnerable category, CWE-120 (Classic Buffer Overflow).

One example of an NVD-CWE-noinfo vulnerability is **CVE-2021-36922**. This vulnerability relates to a USB Utility Driver found in certain Camera/Hub/Audio devices. It allows local low-privileged users to gain unauthorized access to USB devices by sending a specially crafted Device IO Control packet.

In the **Health** class, an interesting observation is the absence of buffer overflow errors. However, authentication and cryptographic problems are prominent. The main vulnerability types within the Health class include CWE-287 (Improper Authentication) and CWE-620 (Unverified Password Change), which are authentication-related issues, and CWE-321 (Use of Hard-coded Cryptographic Key), which is a cryptography problem.

The last two kinds are **Toy** and **Peripheral** classes. Six types of vulnerabilities are detected from 4 vendors.

- CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer.
- CEW-120:Classic Buffer Overflow.

[14] https://www.fujitsu.com/global/
[15] https://www.realtek.com/en/
[16] https://www.synology.com/en-global

- CWE-306:Missing Authentication for Critical Function.
- CWE-427:Uncontrolled Search Path Element
- CWE-732:Incorrect Permission Assignment for Critical Resource.
- NVD-CWE-Other

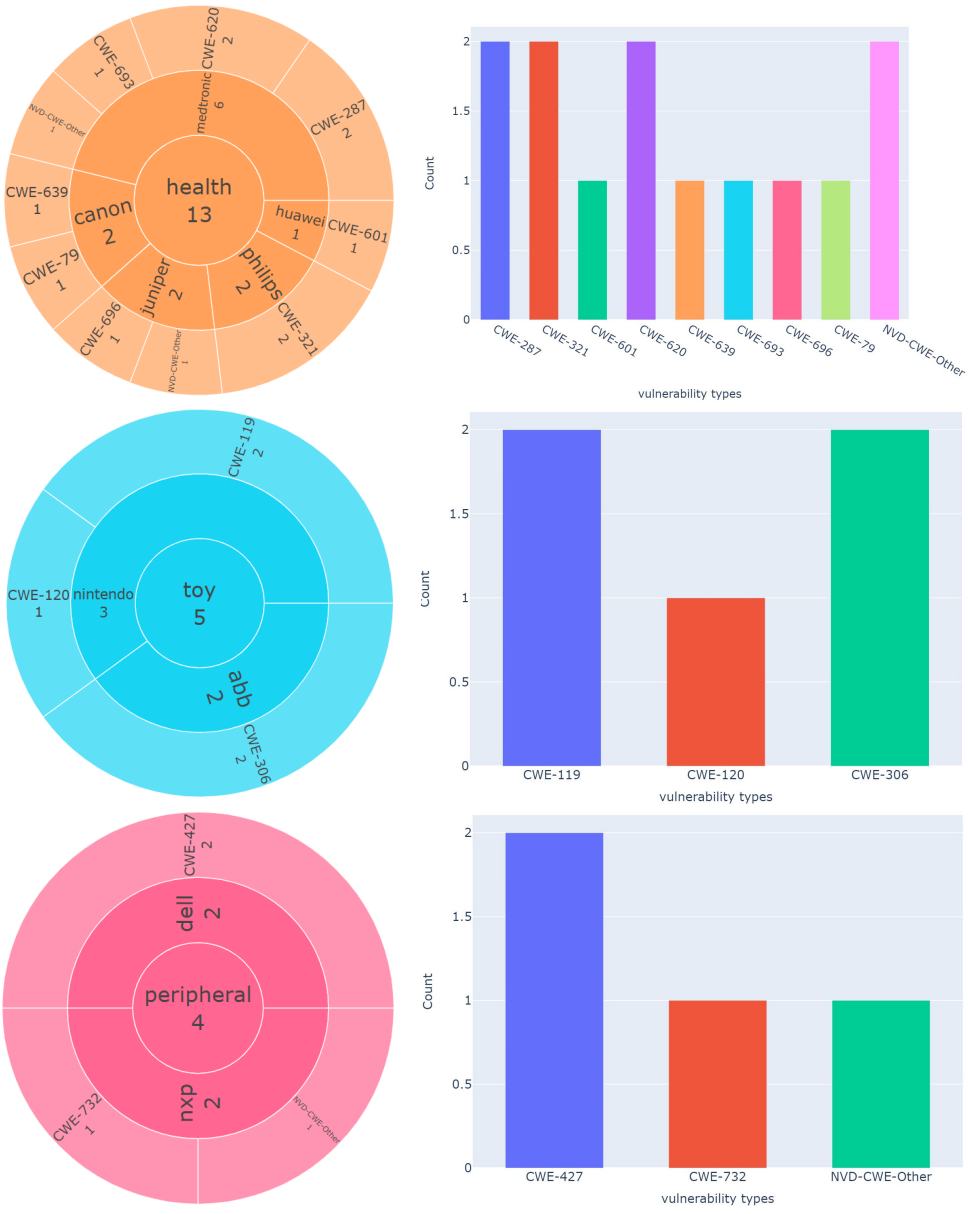

Figure 15: Vulnerabilities of Health, Toy and Peripheral class devices via types

3.3 Severity of Vulnerabilities

Based on the assessment using CVSS v3 (Figure 16), it is evident that a significant portion of vulnerabilities falls under the CRITICAL and HIGH-risk levels, accounting for more than

half of the total vulnerabilities detected.[17]

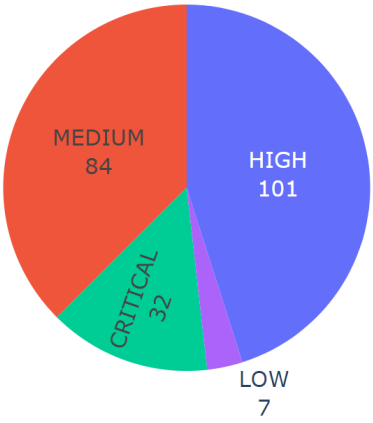

Figure 16: Vulnerability of Bluetooth devices by risk level from 2021(CVSS v3)

For the **Imaging** class, the vulnerabilities are mainly concentrated in the HIGH and MEDIUM risk levels, with 45 and 34 vulnerabilities respectively. CRITICAL-level vulnerabilities account for only 4, while LOW-level vulnerabilities amount to 3. Among the HIGH-level vulnerabilities, 16 are contributed by Nvidia, while Bosch and Realtek each have 8 vulnerabilities. Nvidia is the sole vendor with vulnerabilities in the LOW risk level. The 4 CRITICAL vulnerabilities are attributed to Bosch (3) and Flir (1)[18].

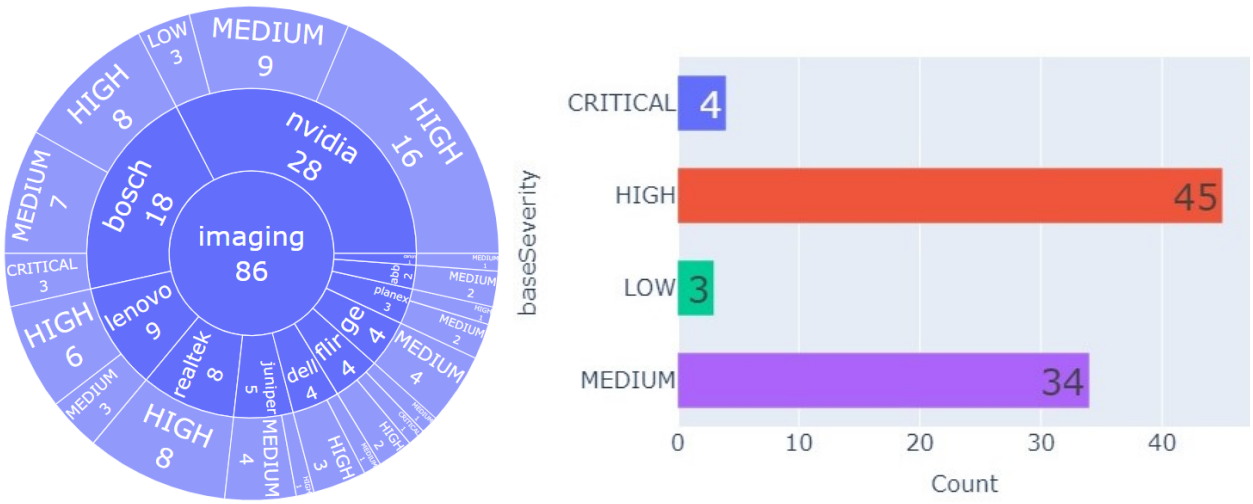

Figure 17: Vulnerabilities of Imaging class devices via severity

One example of a CRITICAL vulnerability is **CVE-2022-37061**, which pertains to Flir. This vulnerability, rated with a risk score of 9.8, affects FLIR AX8 thermal sensor cameras up to version 1.46.16. The vulnerability, known as Remote Command Injection, allows attackers

[17]Notice: The number of vulnerabilities in this subsection may differ from the previous subsection3.2 due to variations in CVE and CWE mappings.

[18]`https://www.flir.com/products/ax8-automation/`

to inject commands through the "id" parameter in the "res.php" endpoint. Exploiting this flaw grants unauthorized access and root privileges, enabling the attacker to assume complete control over the camera's operating system.

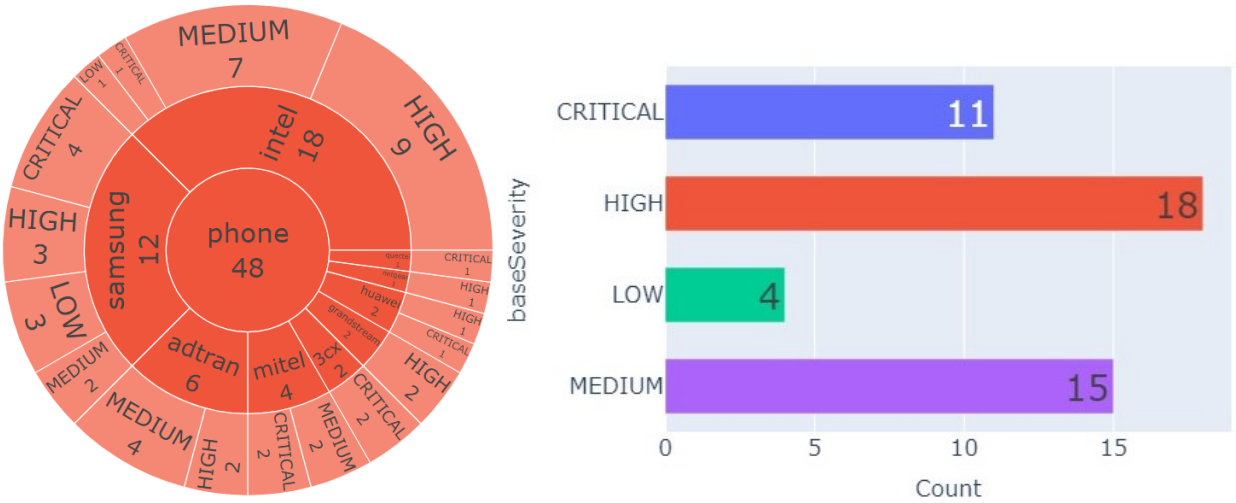

Figure 18: Vulnerabilities of Phone class devices via severity

The **Phone** class exhibits 18 vulnerabilities classified as MEDIUM level, 15 vulnerabilities classified as HIGH level, and 11 vulnerabilities classified as CRITICAL level.

Among the HIGH-level vulnerabilities, half of them are found in Intel products. Specifically, there are 4 CRITICAL vulnerabilities from Samsung, while Mitel[19] and 3cx[20] each has 2 CRITICAL vulnerabilities.

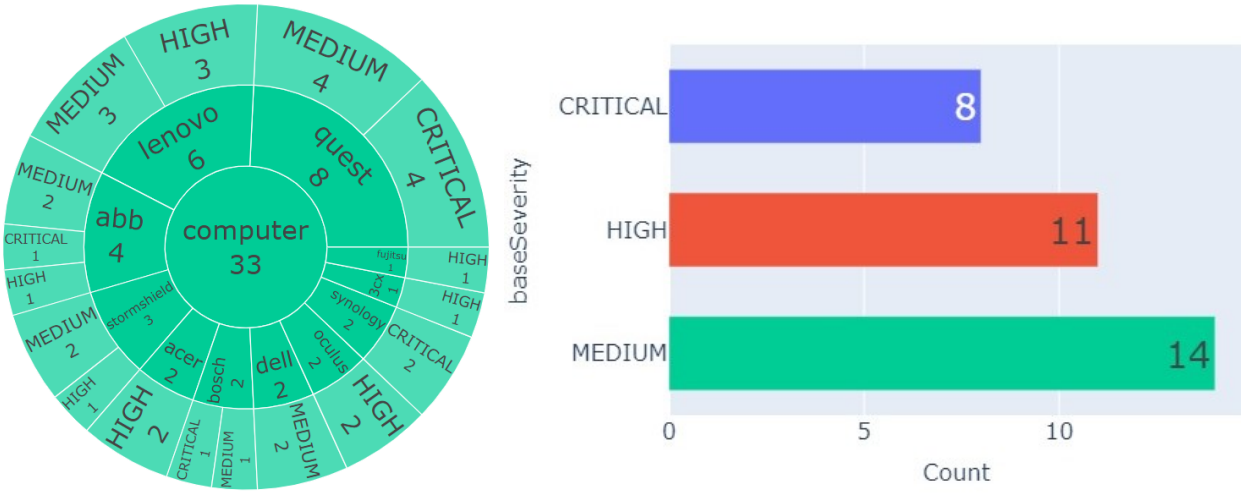

Figure 19: Vulnerabilities of Computer class devices via severity

For **Computer** class, no LOW-level vulnerabilities exist. And CRITICAL weaknesses come

[19] https://www.mitel.com/
[20] https://www.3cx.com/

from 4 vendors: Quest, Synology, Bosch and ABB, and half of the CRITICAL vulnerabilities belong to Quest, half of MEDIUM vulnerabilities come from Lenovo and Quest.

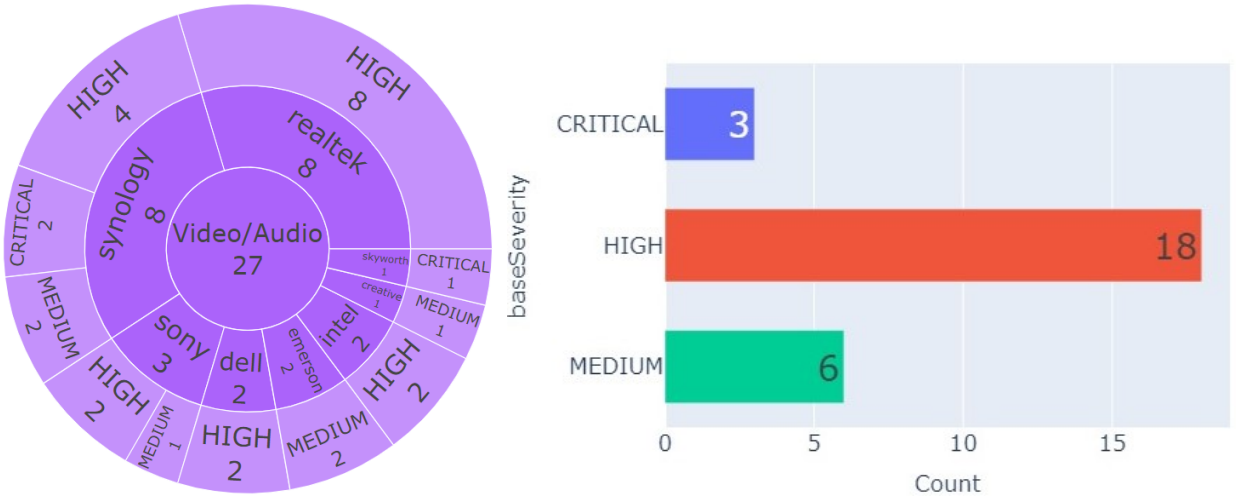

Figure 20: Vulnerabilities of Video/Audio class devices via severity

For the **Video/Audio** class, the vulnerabilities mainly fall into the HIGH risk level, with approximately half of them attributed to Realtek. One example of a CRITICAL vulnerability from Realtek is **CVE-2021-41873**, which has a risk score of 10.0. This vulnerability affects the Penguin Aurora TV Box 41502, a high-end network HD set-top box developed by Tencent Video and Skyworth Digital. It involves an unauthorized access vulnerability, enabling attackers to gain remote control of the TV without proper authorization.

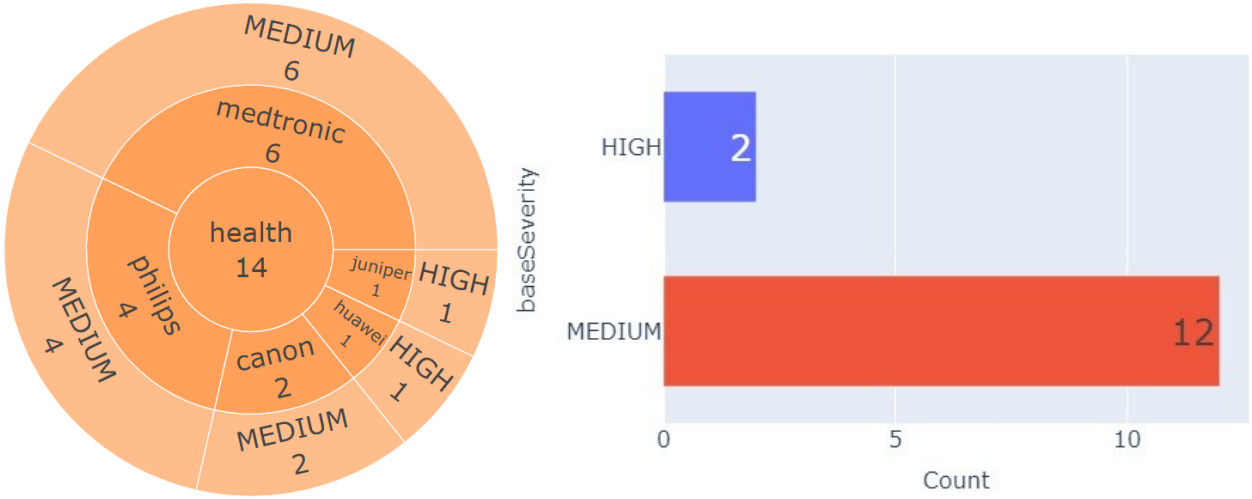

Figure 21: Vulnerabilities of Health class devices via severity

Fortunately, the **Health** devices have no vulnerabilities classified as CRITICAL level. Only two weaknesses are categorized as HIGH level, which are associated with vendors Juniper Networks and HUAWEI.

Regarding the **Toy** class and **Peripheral** class, the risk level distribution is illustrated in Figure 22 and Figure 23 respectively. These figures provide an overview of the vulnerability risk levels for these device classes.

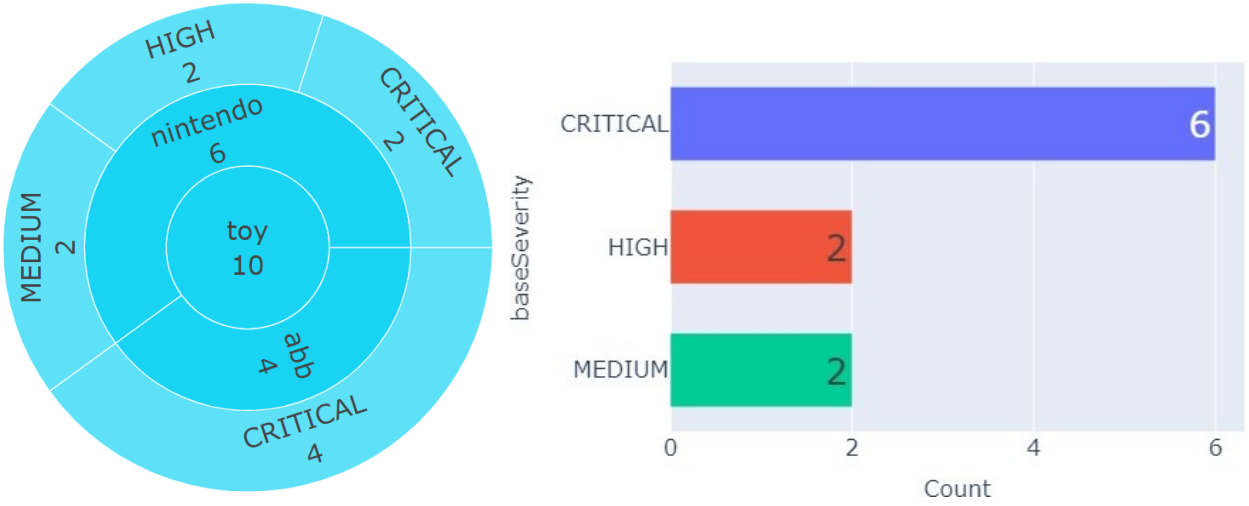

Figure 22: Vulnerabilities of Toy class devices via severity

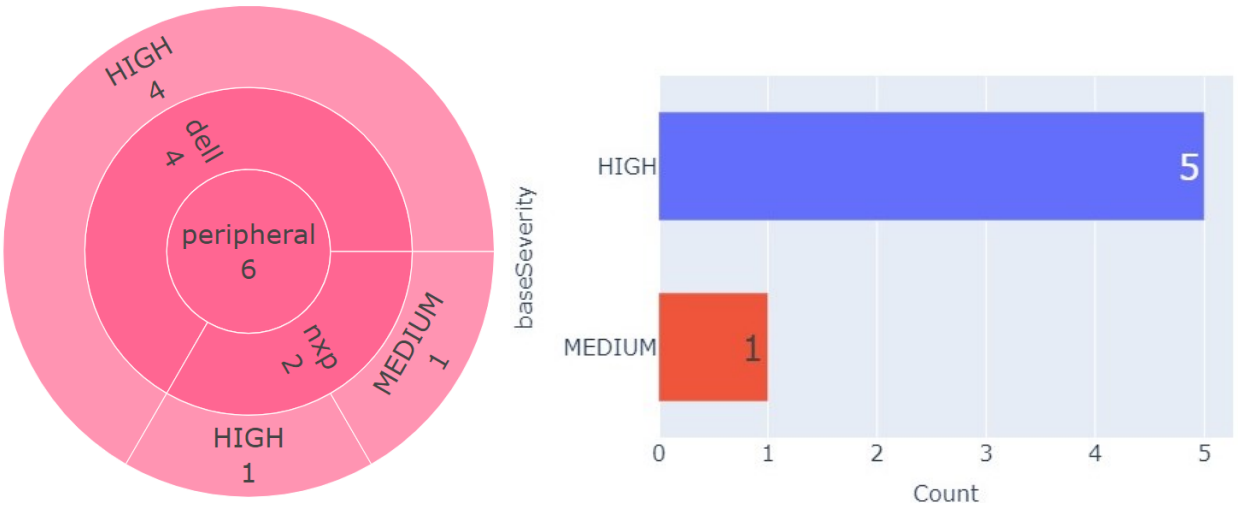

Figure 23: Vulnerabilities of Peripheral class devices via severity

4 Vulnerabilities of WiFi

In this section, we will provide statistics on vulnerabilities in Wi-Fi devices. We will begin by gathering the necessary information, which will serve as keywords for extracting relevant vulnerabilities. Subsequently, we will analyze the severity and risk levels of vulnerabilities based on vendors in subsections 4.2 and 4.3, respectively. It is important to note that while we cannot categorize the information according to specific Wi-Fi protocols, we will mention companies associated with unsecured Wi-Fi protocols in these subsections to highlight the potential vulnerabilities of such protocols.

4.1 Overview

bssid	ssid	equenc	capabilities	lasttime	lastlat	lastlon	type
Filter	Filter	Filter	Filter	Filter	Filter	Filter	W
cc:db:...	eduroam	2462	[WPA2-EAP/SHA...	1676465070711	55.78954...	12.5251167248742	W
cc:db:...	device	2462	[ESS]	1676469851806	55.78955...	12.525143066728	W
cc:db:...	DTUsecure	2462	[WPA2-EAP/SHA...	1676465070711	55.78954...	12.5251167248742	W
cc:db:...	DTUguest	2462	[ESS]	1676469851806	55.78955...	12.525143066728	W
cc:db:...	DTUguest	2412	[ESS]	1676469851806	55.78955...	12.525143066728	W
cc:db:...	device	2412	[ESS]	1676469851806	55.78955...	12.525143066728	W
cc:db:...	eduroam	2437	[WPA2-EAP/SHA...	1676462363751	55.7895662	12.5250856	W

Figure 24: WiFi data in WiGLE

To produce statistics on WiFi devices, and find useful information to help us search for vulnerabilities in those WiFi devices, we analyse the information statistically. Picture 24 displays the useful information in our experiment. The capabilities field provides WiFi encryption protocol, ciphers and other protocols used by devices.

Encryption	Count	Percentage
Open Access	13463	7.84
UNKNOWN	17998	10.47
WEP	8324	4.85
WPA	4519	2.63
WPA2	108861	63.41
WPA3	219	0.13
TOTAL	191743	1

Table 2: WiFi encryption protocol

Table 2 presents the statistical results of WiFi encryption methods. The majority of networks

(63.41%) utilize the WPA2 encryption method. Open WiFi networks account for the second largest portion (7.84%), excluding unknown networks. Surprisingly, a considerable number of networks still employ the deprecated WEP protocol. Additionally, 2,935 networks are found to be using the insecure WPA-TKIP[2] encryption protocol.

Cipher	Count
PSK	86943
EAP/SHA1	9313
PSK+FT/PSK	1416
EAP/SHA1+FT/EAP	738
PSK+SAE	672
SHA256	140
EAP/SHA1+?	79
SAE	62
SHA256+SAE	34
EAP/SHA1+EAP/SHA256	32
PSK+FT/PSK+SAE+FT/SAE	9
EAP/SHA1+?+FT/EAP	8

Table 3: Key management and Hash

According to the statistical results, the Pre-Shared Key (PSK) cipher is the most widely used encryption method, with 86,943 networks detected. However, it is worth noting that a significant number of networks still use the SHA1 cipher, especially in university networks like eduroam. These findings highlight the importance of transitioning to more secure encryption methods and phasing out the usage of deprecated protocols.

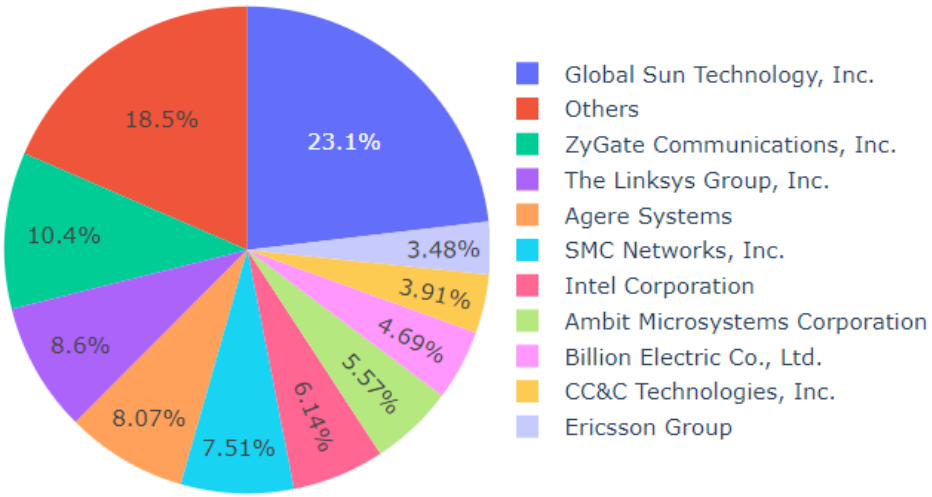

Figure 25: Vendors of open WiFi

Figure 25 presents the distribution of open Wi-Fi networks among different companies. It is evident that Global Sun holds the largest share of open Wi-Fi networks with a percentage of 23.1%. Additionally, Figure 26 illustrates the distribution of WEP Wi-Fi products among vendors, where Global Sun again dominates with a share of 24.4%.

Furthermore, among the top 10 vendors, ZyGate, Linksys, Agere, SMC, CC&C, and Billion are also found to have both WEP Wi-Fi and open Wi-Fi networks in their portfolios. For a comprehensive list of vendors associated with open Wi-Fi and WEP Wi-Fi networks, please refer to Appendix 5.

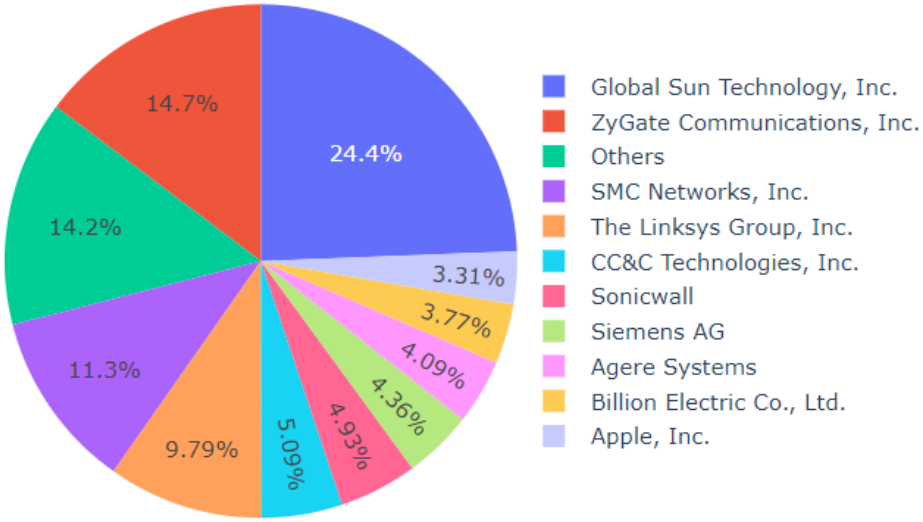

Figure 26: Vendor of WEP Wi-Fi

4.2 Types of Vulnerabilities

Heatmap 27 presents a comprehensive overview of detected vulnerabilities in WiFi devices, encompassing the top 22 distinct types of vulnerabilities.

Examining the x-axis, we observe a decreasing trend in the number of vulnerabilities among the 22 categories. Notably, **Improper Input Validation** emerges as the most prevalent vulnerability, exclusively associated with Intel. Following closely are **Out-of-bounds Write** and **Out-of-bounds Read** vulnerabilities, both classified as **Buffer Overflow** instances. Equally noteworthy is the presence of the 6th most prevalent vulnerability, **Classic Buffer Overflow**, and the 23rd vulnerability, **Stack-based Buffer Overflow**, both attributable to buffer overflow scenarios. Additional common vulnerabilities include **CSRF** (Cross-Site Request Forgery) and **Cross-site Scripting**.

Turning our attention to the y-axis, vendors are ranked based on the number of vulnerabilities attributed to each. Intel, a prominent IT company, exhibits the highest vulnerability count, with a total of 94 reported vulnerabilities in 2021. Of these, 59 vulnerabilities are associated with improper input validation. MediaTek Inc. follows closely with 36 vulnerabilities, all

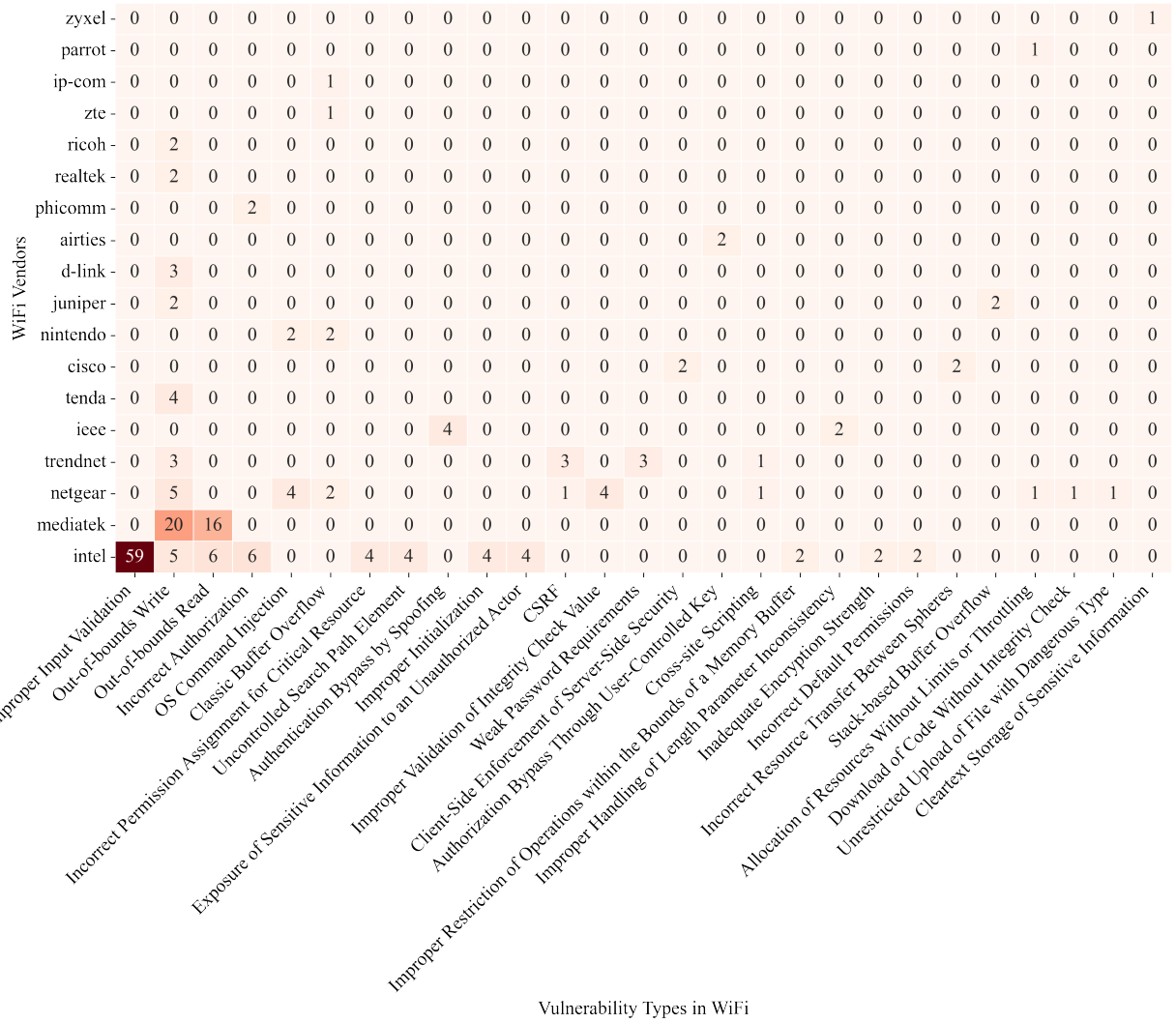

Figure 27: Vulnerabilities of WiFi devices

classified as buffer overflow issues. Subsequently, vendors ranging from Airties[21] to Ricoh[22] each possess two vulnerabilities, while Zte[23] to Zyxel[24] have a single vulnerability each.

In addition, we can extract specific subsets from the heatmap, specifically vendors that utilize the WEP (Wired Equivalent Privacy) Wi-Fi protocol and those that offer open Wi-Fi networks. Referring back to the analysis provided in the overview section (see 4.1), we find

[21] https://airties.com/
[22] https://www.ricoh.com/
[23] https://ztedevices.com/en-gl/
[24] https://www.zyxel.com/global/en

that vendors such as Intel, Netgear[25], Tenda[26], Cisco[27], and D-link[28] are associated with Wi-Fi devices employing the WEP protocol. Figure 28 illustrates the vulnerabilities associated with these companies. It should be noted that not all Wi-Fi devices from these vendors utilize WEP, hence the identified vulnerabilities are considered potential vulnerabilities in devices utilizing WEP Wi-Fi.

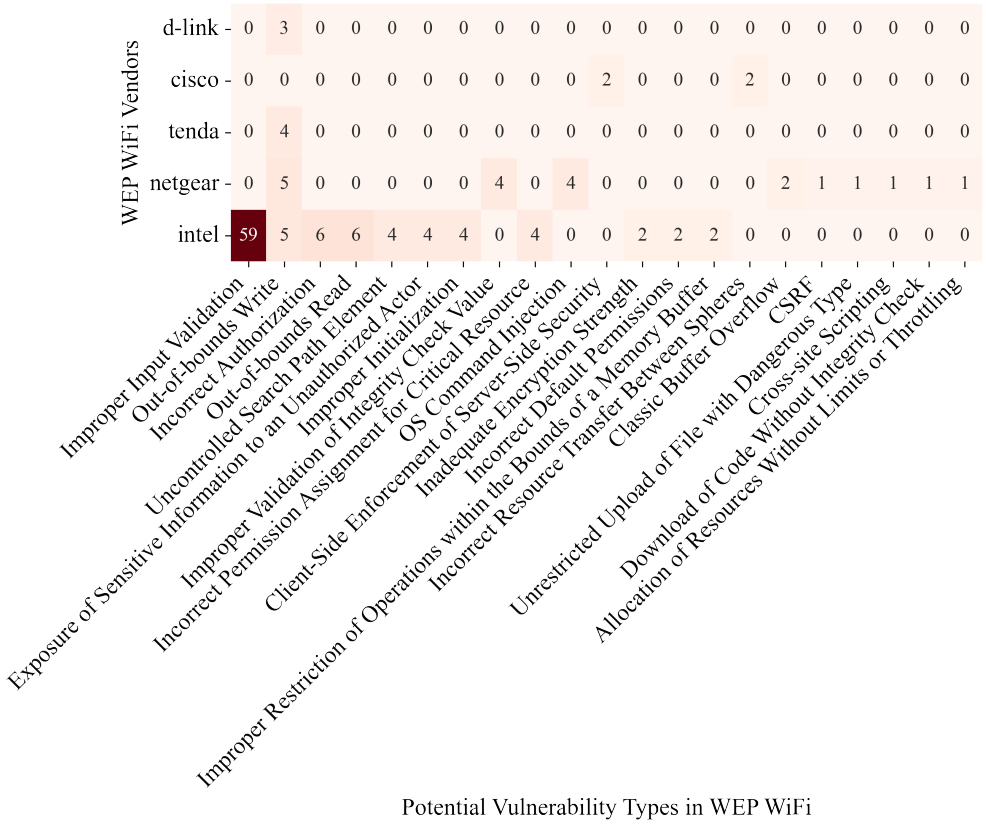

Figure 28: Potential vulnerabilities of WEP Wi-Fi via types

Same with WEP Wi-Fi, we extract those vendors who have open Wi-Fi in heatmap 27 as a subset. Picture 29 shows the potential vulnerabilities that exist in devices using open Wi-Fi. Obviously, 13 types of vulnerabilities may exists in open Wi-Fi devices

Here are some examples of vulnerabilities found in WiFi devices:

- **CVE-2022-21181**: This vulnerability relates to an improper input validation issue with a severity score of 7.8 (high) and is specific to Intel. It has been discovered that certain WiFi products possess the capability to elevate the privileges of a privileged user through local access.

[25] https://www.netgear.com/
[26] https://www.tendacn.com/search/Wi-Fi%207.html
[27] https://www.cisco.com/site/us/en/index.html
[28] https://eu.dlink.com/dk/da

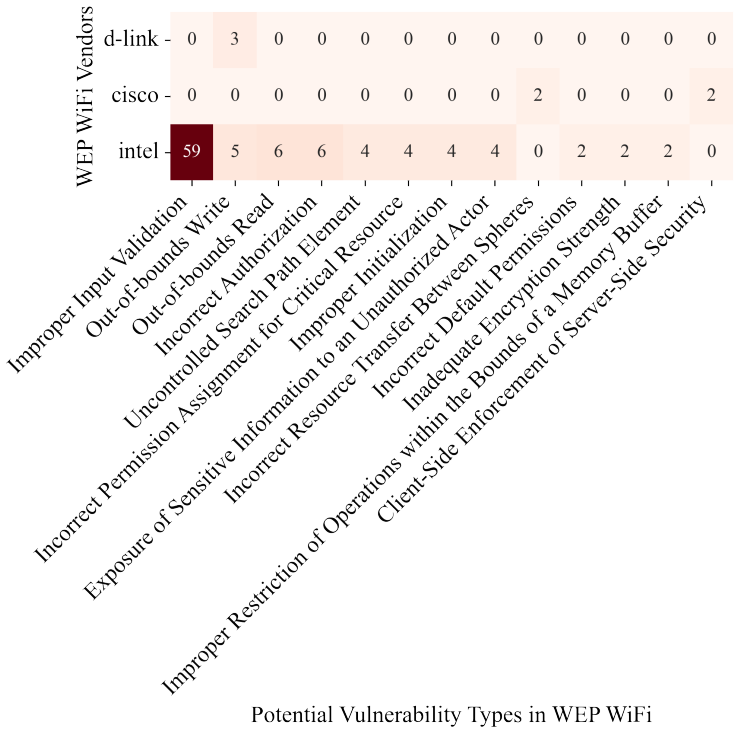

Figure 29: Potential vulnerabilities of Open Wi-Fi via types

- **CVE-2021-35055**: This vulnerability is classified as an out-of-bounds write vulnerability with a risk score of 8.8 (high) and is associated with MediaTek Inc. The microchips utilized in their devices lack proper bounds checking, which could be exploited by malicious actors to escalate their privileges.
- **CVE-2021-23168**: This vulnerability pertains to out-of-bounds read vulnerabilities and carries a risk score of 6.5 (high). It affects Intel devices and could potentially be exploited by an unauthorized user in close proximity to the affected device, enabling them to cause a denial of service.

4.3 Severity of Vulnerabilities

Picture 30 illustrates the distribution of vulnerabilities in Wi-Fi devices according to their severity levels. Notably, the majority of vulnerabilities, accounting for 53.5% (138), are classified as HIGH level. On the other hand, a minimal percentage of vulnerabilities, just 0.775% (2), are categorized as LOW level.

Examining the specific distribution of severity levels among Wi-Fi devices, as presented in Figure 31, it is evident that Mediatek firm accounts for more than half of the high-level vulnerabilities. Additionally, Intel and Netgear contribute 36 and 14 vulnerabilities, respectively. Regarding the MEDIUM level vulnerabilities, the majority, approximately 78.2% (68), are associated with Intel products. LOW-level vulnerabilities are exclusive to

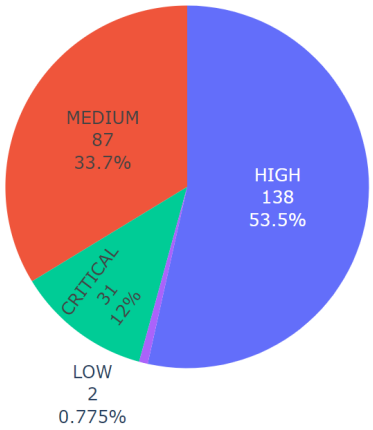

Figure 30: Vulnerability of Wi-Fi devices by risk level from 2021(CVSS v3)

Intel devices, while CRITICAL-level vulnerabilities are detected in an average of 11 different vendors.

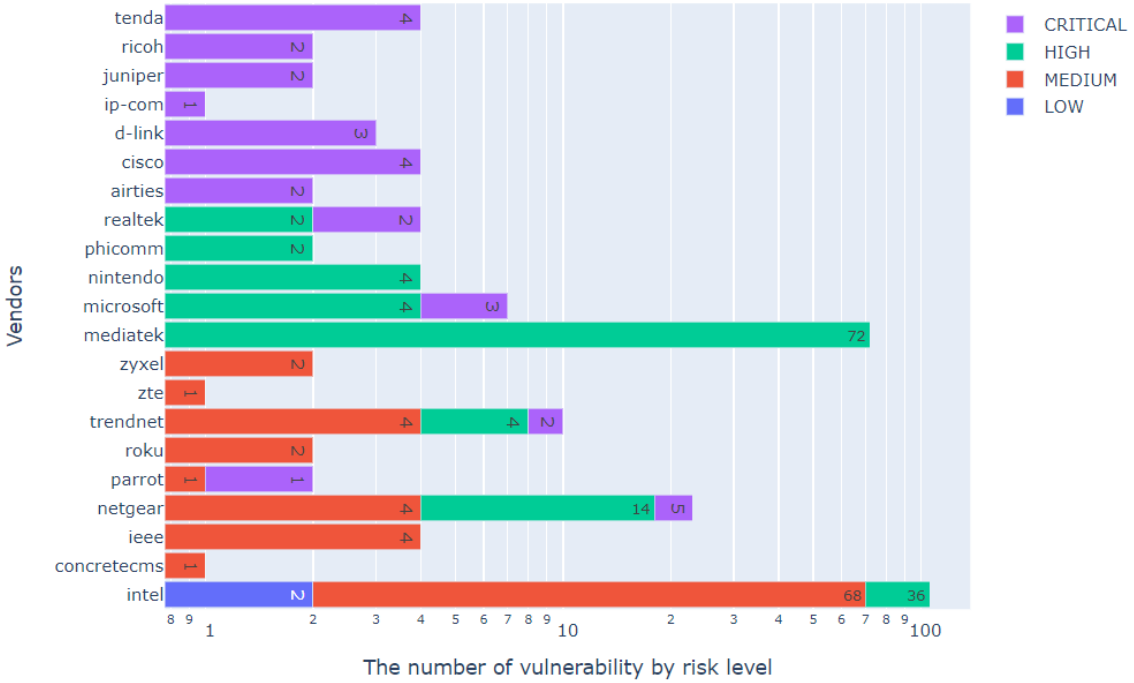

Figure 31: The number of vulnerabilities in different WiFi vendors by risk level(CVSS v3)

There are some examples of each Wi-Fi devices vulnerabilities:

- **CVE-2023-27012** is a critical (9.8) Out-of-bounds Write vulnerability found in the Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn router. This vulnerability allows attackers to execute arbitrary code or initiate a Denial of Service (DoS) attack by exploiting the stack overflow vulnerability in the setSchedWifi function.
- **CVE-2021-39306:** This is a critical vulnerability with a severity score of 9.8, affecting

Realtek. It involves a stack buffer overflow in the Realtek RTL8195AM device prior to version 2.0.10. The vulnerability resides in the client code and can be exploited by an attacker who sends a large-sized Authentication challenge text within the context of WEP security.

- **CVE-2022-34326:** This is a HIGH-level vulnerability affecting Realtek products. In the ambiot amb1_sdk (SDK for Ameba1) before 2022-06-20, on Realtek RTL8195AM devices a vulnerability was discovered. It involves Soft AP mode, where repeated failures in the Wi-Fi connection (specifically, four-way handshake failures) can lead to the locking of the timer task and RX task.
- **CVE-2022-39067:** It is a MEDIUM-level (6.5) vulnerability affecting ZTE. The ZTE MF286R device is vulnerable to a buffer overflow. Insufficient input validation on parameters of the Wi-Fi interface enables an authenticated attacker to exploit this vulnerability and launch a denial of service attack.
- **CVE-2021-23188** is a LOW-level(3.3) vulnerability in Intel products, where improper access control may result in potential information disclosure through local access.

Similarly, we further analyze two subsets of Wi-Fi networks: WEP Wi-Fi and open Wi-Fi, as depicted in Figure 32 and Figure 33, respectively. These graphs allow us to discern the distribution of potential vulnerabilities associated with each type of Wi-Fi network, with a particular focus on the risk levels.

Analyzing these graphs, we observe that the potential vulnerabilities associated with both WEP Wi-Fi and open Wi-Fi networks predominantly fall within the MEDIUM risk level. This concentration of potential vulnerabilities can be attributed to the presence of Intel, which has 11.7% open Wi-Fi devices, as a prominent vendor within these networks.

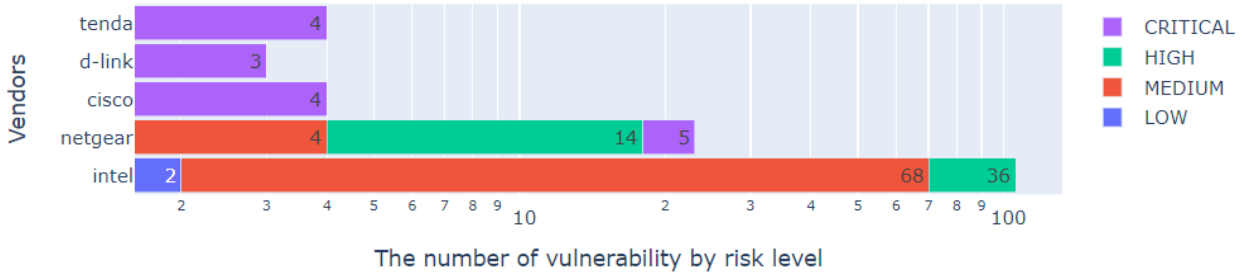

Figure 32: Potential vulnerabilities of WEP Wi-Fi via risk level

Figure 33: Potential vulnerabilities of Open Wi-Fi via risk level

5 Discussion

By leveraging a dataset consisting of more than 1 million Bluetooth and Wi-Fi data, we have significantly enhanced our understanding of IoT network devices. Our analysis of keywords in the Overview subsections highlights the importance of these keywords in gaining insights into Bluetooth and Wi-Fi networks. Through the utilization of these keywords, we have collected vulnerabilities pertaining to Bluetooth and Wi-Fi networks. The inclusion of CVEs in this paper further ensures the accuracy and reliability of our statistical findings.

However, we acknowledge that further research conducted with our extensive database can further enhance the comprehensiveness and refinement of our results.

A. Optimize Vendor Names: To utilize vendor names as keywords, we employed filtering techniques to remove unnecessary suffixes, prefixes(e.g., *SYSTEMS*, *LTD*, *LIMITED*, *CORPORATION*), and address names. However, with 2608 vendors detected during the Wardriving process, manually verifying each vendor name within the given time constraints proved impractical. Consequently, the vendor names used in the OpenCVE API might contain inaccuracies, potentially leading to gaps in vulnerability data.

	id	published	lastModified	vulnStatus	description_value	keywords
	Filter	Filter	Filter	Filter	AirTies_Air	Filter
1	CVE-2019-6967	2019-03-21T16:01:10.297	2019-03-22T13:25:15.983	Analyzed	Los dispositivos AirTies Air5341 ...	airties
2	CVE-2019-6967	2019-03-21T16:01:10.297	2019-03-22T13:25:15.983	Analyzed	AirTies Air5341 1.0.0.12 devices allo...	airties
3	CVE-2018-17594	2018-10-02T18:29:02.147	2018-11-15T18:54:46.343	Analyzed	Los dispositivos AirTies Air 5443v2 co...	airties
4	CVE-2018-17594	2018-10-02T18:29:02.147	2018-11-15T18:54:46.343	Analyzed	AirTies Air 5443v2 devices with softw...	airties
5	CVE-2018-17593	2018-10-02T18:29:02.053	2018-11-15T18:55:11.483	Analyzed	Los dispositivos AirTies Air 5453 con ...	airties
6	CVE-2018-17593	2018-10-02T18:29:02.053	2018-11-15T18:55:11.483	Analyzed	AirTies Air 5453 devices with software...	airties
7	CVE-2018-17591	2018-10-02T18:29:01.947	2018-11-15T18:55:25.737	Analyzed	Los dispositivos AirTies Air 5453 con l...	airties
8	CVE-2018-17591	2018-10-02T18:29:01.947	2018-11-15T18:55:25.737	Analyzed	AirTies Air 5343v2 devices with softw...	airties
9	CVE-2018-17590	2018-10-02T18:29:01.837	2018-11-15T18:55:35.813	Analyzed	Los dispositivos AirTies Air 5442 con l...	airties
10	CVE-2018-17590	2018-10-02T18:29:01.837	2018-11-15T18:55:35.813	Analyzed	AirTies Air 5442 devices with software...	airties
11	CVE-2018-17589	2018-10-02T18:29:01.743	2018-11-15T19:59:52.337	Analyzed	Los dispositivos AirTies Air 5650 con ...	airties
12	CVE-2018-17589	2018-10-02T18:29:01.743	2018-11-15T19:59:52.337	Analyzed	AirTies Air 5650 devices with software...	airties
13	CVE-2018-17588	2018-10-02T18:29:01.633	2018-11-15T19:59:08.083	Analyzed	Los dispositivos AirTies Air 5650 con l...	airties
14	CVE-2018-17588	2018-10-02T18:29:01.633	2018-11-15T19:59:08.083	Analyzed	AirTies Air 5021 devices with software...	airties
15	CVE-2018-17587	2018-10-02T18:29:01.523	2018-11-15T20:04:43.393	Analyzed	Los dispositivos AirTies Air 5750 con l...	airties
16	CVE-2018-17587	2018-10-02T18:29:01.523	2018-11-15T20:04:43.393	Analyzed	AirTies Air 5750 devices with software...	airties
17	CVE-2015-2797	2015-06-19T14:59:00.067	2016-12-03T03:06:27.040	Modified	Stack-based buffer overflow in AirTies...	airties
18	CVE-2015-2797	2015-06-19T14:59:00.067	2016-12-03T03:06:27.040	Modified	Desbordamiento de buffer basado en ...	airties
19	CVE-2014-100...	2015-01-13T15:59:33.257	2017-09-08T01:29:02.497	Modified	Vulnerabilidad de XSS en top.html en ...	airties
20	CVE-2014-100...	2015-01-13T15:59:33.257	2017-09-08T01:29:02.497	Modified	Cross-site scripting (XSS) vulnerabilit...	airties
21	CVE-2012-0902	2012-01-20T17:55:02.487	2017-08-29T01:31:05.617	Modified	AirTies Air 4450 v1.1.2.18 permite a ...	airties
22	CVE-2012-0902	2012-01-20T17:55:02.487	2017-08-29T01:31:05.617	Modified	AirTies Air 4450 1.1.2.18 allows remot...	airties

Figure 34: Vulnerabilities containing the keyword *AirTies_Air*

B. Optimize Keywords: Some SSIDs provide valuable information about device types, products, and versions, which can be used as keywords to search for vulnerabilities. For instance, devices from AirTies Wireless Networks use SSIDs like *AirTies_Air...* for their Wi-Fi products. Figure 34 illustrates the vulnerabilities identified using the keyword *AirTies_Air*.

Fortunately, all of these vulnerabilities were discovered before 2019 and do not impact our current results. However, due to a large number of Wi-Fi SSIDs (34186), manual extraction of each one is not feasible within the given time frame.

C. Optimize Vulnerability Extraction: It is important to note that a single CWE ID can be assessed by multiple metrics and classified as different weakness types. Additionally, vulnerabilities may have multiple language versions, which can affect the accuracy of our results. Thus, our future work will focus on addressing the challenge of defining the number of CWEs and filtering out duplicate CWEs resulting from variable language versions.

D. Provide More Detailed Analysis: By using SSIDs as keywords, we can extract additional vulnerabilities from the CVE database, allowing for a more in-depth analysis of risk severity for each vulnerability type.

E. Filter improper keywords The process of filtering improper keywords is crucial to accurately categorize vulnerabilities. While using specific keywords for vulnerability searches, Minimizing unrelated vulnerabilities is essential for accurate classification based on keywords. For example, if the keyword "health" is used for Bluetooth vulnerability searches, vulnerabilities containing terms such as "BatteryHealth" may be mistakenly considered as part of the "Health" class, even if they are not relevant to the defined health-related devices in the context of the paper. Therefore, careful evaluation and filtering are necessary to maintain the accuracy of vulnerability classification.

6 Conclusion

This report provides a comprehensive overview of the security issues and vulnerabilities present in local IoT devices. By analyzing over 1 million network data of Bluetooth and Wi-Fi, we have identified key findings that shed light on the security landscape of IoT devices.

Our findings indicate that buffer overflow, cross-site scripting, and authentication-related problems are the most frequent vulnerabilities found in both Bluetooth and Wi-Fi devices. These vulnerabilities pose significant risks to the security and integrity of IoT ecosystems.

Furthermore, we observed that the majority of vulnerabilities in both Bluetooth and Wi-Fi networks are categorized as HIGH severity, followed by MEDIUM and CRITICAL levels. The number of LOW-level vulnerabilities is relatively low, suggesting that there is a need for increased attention to security practices in IoT devices.

In the case of Bluetooth devices, we classified them into 7 distinct majority classes, each with its own unique risk types and severity levels. This highlights the diversity and complexity of vulnerabilities present in Bluetooth-enabled IoT devices.

For Wi-Fi devices, we provided an overview of the vulnerabilities associated with them. Additionally, we focused on devices that use the WEP protocol or lack encryption, extracting subsets of vulnerabilities specific to these devices. This highlights the potential risks and vulnerabilities that may exist in these particular Wi-Fi devices.

In the Discussion section, we presented four optimization methods that can be employed for further investigation and improvement in IoT device security.

To ensure the security and privacy of IoT devices, it is crucial for organizations and individuals to actively collaborate with industry experts, adhere to security best practices, and stay updated on emerging threats. By adopting robust security measures, conducting regular vulnerability assessments, and promoting ongoing awareness, we can effectively safeguard IoT devices and protect the integrity of the connected environment.

References

[1] C. Home, "Assigned Numbers Bluetooth Document."

[2] V. O. Etta, A. Sari, A. L. Imoize, P. K. Shukla, and M. Alhassan, "Assessment and test-case study of wi-fi security through the wardriving technique," *Mobile Information Systems*, vol. 2022, 2022.

7 Appendix A

7.1 Vulnerabilities of Bluetooth

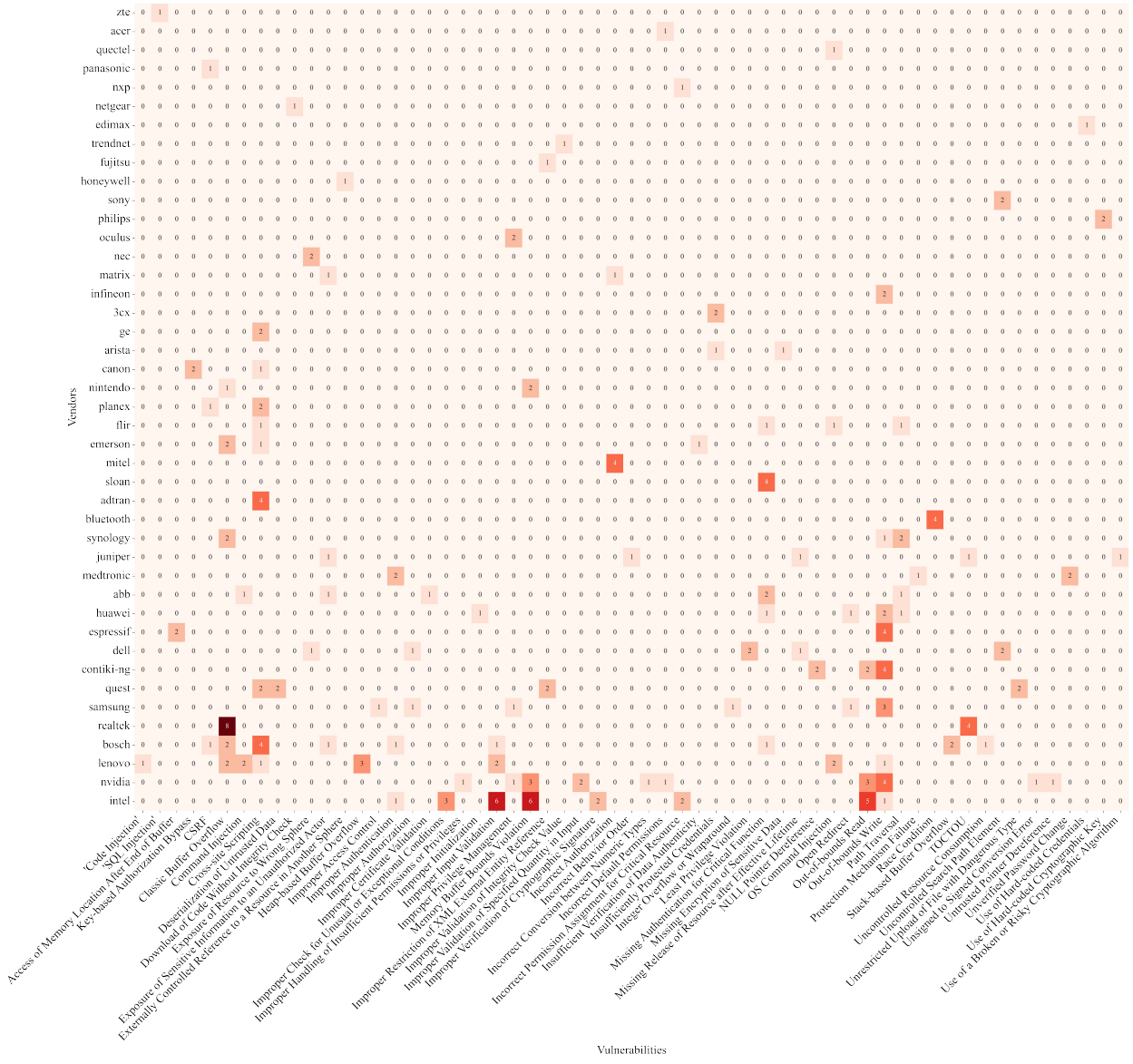

Figure 35: Entire vulnerabilities of Bluetooth

7.2 WEP Wi-Fi vendors

Company	Count	Company	Count
Global Sun Technology, Inc.	1370	ZyGate Communications, Inc.	828
SMC Networks, Inc.	633	The Linksys Group, Inc.	550
CC&C Technologies, Inc.	286	Sonicwall	277
Siemens AG	245	Agere Systems	230
Billion Electric Co., Ltd.	212	Apple, Inc.	186
3COM	86	Tilgin AB	80
Intel Corporation	79	Cisco Systems, Inc.	74
XEROX CORPORATION	49	D-LINK SYSTEMS, INC.	47
Extreme Networks, Inc.	43	NETGEAR	37
Prime Electronics & Satellitics Inc.	34	Colubris Networks	27
Hewlett Packard	22	Ambit Microsystems Corporation	22
BUFFALO.INC	19	Acer Incorporated	17
AVM GmbH	17	CyberTAN Technology Inc.	16
Shanghai MXCHIP Information Technology Co., Ltd.	15	Bromax Communications, Ltd.	15
Senao International Co., Ltd.	13	Ericsson Group	13
Aceex Corporation	12	Runtop, Inc.	7
Tellus Group Corp.	5	PRO-NETS Technology Corporation	5
Air Link Technology	5	ASUSTek COMPUTER INC.	4
XAVi Technologies Corp.	3	Qisda Corporation	3
SURECOM Technology Co.	2	MINIWARE TECHNOLOGY	2
LITE-ON Communications, Inc.	2	Enterasys	2
ARRIS Group, Inc.	2	XIRCOM	1
W-Link Systems, Inc.	1	Ubiquiti Inc	1
Tenda Technology Co.,Ltd.Dongguan branch	1	TECOM Co., Ltd.	1
Sena Technologies, Inc.	1	SUREMAN COMP. & COMMUN. CORP.	1
Ruckus Wireless	1	Puretek Industrial Co., Ltd.	1
Netspect Technologies, Inc.	1	NEC Corporation	1
Murata Manufacturing Co., Ltd.	1	HCL LIMITED	1
Freecom Technologies GmbH	1	Compal Electronics INC.	1
COMPU-SHACK ELECTRONIC GMBH	1	BMT Medical Technology s.r.o.	1
Allied Data Technologies	1	ALPSALPINE CO,.LTD	1
ACCTON TECHNOLOGY CORP.	1	7INOVA TECHNOLOGY LIMITED	1

7.3 Open Wi-Fi vendors

Vendors	count	Vendors	count
Global Sun Technology, Inc.	1017	Murata Manufacturing Co., Ltd.	6
ZyGate Communications, Inc.	457	W-Link Systems, Inc.	5
The Linksys Group, Inc.	378	Ubiquiti Inc	5
Agere Systems	355	Tellus Group Corp.	5
SMC Networks, Inc.	330	LITE-ON Communications, Inc.	5
Intel Corporation	270	Qisda Corporation	4
Ambit Microsystems Corporation	245	Runtop, Inc.	3
Billion Electric Co., Ltd.	206	D&M Holdings Inc.	3
CC&C Technologies, Inc.	172	Cellvision Systems, Inc.	3
Ericsson Group	153	BUFFALO.INC	3
Colubris Networks	134	AVM GmbH	3
3COM	83	XAVi Technologies Corp.	2
Prime Electronics & Satellitics Inc	61	SURECOM Technology Co.	2
Cisco Systems, Inc	61	Nexsi Corporation	2
D-LINK SYSTEMS, INC.	55	Zinwell Corporation	1
Apple, Inc.	46	Uniwill Computer Corp.	1
Siemens AG	37	Sena Technologies, Inc.	1
Acer Incorporated	35	SAMSUNG ELECTRO MECHANICS CO., LTD.	1
Hewlett Packard	33	Netspect Technologies, Inc.	1
Philips	31	NEC Corporation	1
XIRCOM	25	Microchip Technology Inc.	1
Roving Networks	23	Makino Milling Machine Co., Ltd.	1
CyberTAN Technology Inc.	20	LOGIC REPLACEMENT TECH. LTD.	1
Bromax Communications, Ltd.	19	LABTAM LIMITED	1
Sonicwall	17	EQUIP'TRANS	1
Senao International Co., Ltd.	15	Creatix Polymedia Ges Fur Kommunikaitonssysteme	1
XEROX CORPORATION	13	CELOX Networks	1
Extreme Networks, Inc.	9	CANON INC.	1
Enterasys	8	Bluegiga Technologies OY	1
Bridgeco Co AG	8	ASANTE TECHNOLOGIES	1
Tilgin AB	7	3COM EUROPE LTD	1
Winmate Communication, Inc.	6		

Table 5: Entire vendors list of op