Analysis of SNMP through Censys Datasets

Ignacy Kępka
University of Twente
Drienerlolaan 15, 7522 NB Enschede
The Netherlands
i.kepka@student.utwente.nl

Abstract

SNMP (Simple Network Management Protocol) is an essential protocol, used worldwide by millions of networking devices i.e., routers, switches, bridges, or even CCTV cameras. Its main purpose is to manage and monitor network devices on the Internet and establish communication between them. It operates on the application layer of the IP Suite and provides a standardized framework for devices to share their operational information with network administrators. SNMP allows administrators to remotely manage network performances, troubleshoot network problems and plan future network expansions. This research will utilize the dataset provided by a cybersecurity company “Censys” to identify the prevalence and distribution of SNMP-enabled devices worldwide, map out SNMP-enabled devices based on their configuration and associated vendors, as well as, determine the scale of potentially vulnerable devices by utilizing search engine Shodan (the first search engine for Internet-connected devices). The results of this analysis were compared with the outcome of another research paper titled “Third time's not a charm: exploiting SNMPv3 for router fingerprinting.” [1]. The results also provided interesting insight into the shift in worldwide vendor dominance on the market between 2021 and 2024. This research is expected to update the results of previous works concerning the mapping of active SNMP devices found in the World Wide Web (WWW) and provide more insight into the potential vulnerabilities found in such devices.

Keywords

SNMP Deployment, SNMP Configuration, SNMP Vulnerabilities, Censys Dataset, Network Systems, Shodan Engine, CVE Database.

1. Introduction

It is difficult to imagine today’s world, without the Internet being invented. Network systems became an irreplaceable part of human interactions between other humans and/or machines. Chatting with friends, scheduling doctor appointments, or purchasing items are just a few examples of how a person uses the Internet. Nevertheless, network systems have a much wider scope of usability, as they provide: communication, access to resources, centralization of data and transfer of files [2]. For those to be attainable, they require fully automated network systems that are interoperable and can easily be managed and diagnosed if needed. Thanks to that a protocol called Simple Network Management Protocol (SNMP) has been developed that would provide the aforementioned functionalities to the network systems. SNMP is essentially a “simple set of operations (and the information these operations gather) that gives administrators the ability to change the state of SNMP-based devices” [3].

With the help of SNMP, administrators can determine a range of information that can prove to be useful in determining the issues that appear in the networks, controlling the workflow of devices in such networks, and optimizing their functionality. It is estimated based on empirical evidence that there are around 27 million [1] devices in the World Wide Web that use the SNMP protocol. Nevertheless, this number has been determined in late 2021. Since it is already getting outdated, it would prove very useful to update the existing knowledge concerning the amount of SNMP-related devices, since the internet is always expanding. It is estimated that between 2021 and 2024 the number of network appliances in the World Wide Web, increased from 21.1 billion to 26.16 billion by the end of 2023 [4]. Out of these 26.16 billion devices, it would be interesting to determine how many of them utilize SNMP protocols, where they are located at, what are the most common vendors, and what kind of vulnerabilities might they be susceptible to.

There were already researches aiming at analyzing how many devices in the World Wide Web use SNMP and how they are being distributed around the world. Each utilizes different concepts of actively searching for such devices, with a unique approach, but a very similar goal. One group of researchers used the unintended functionality of SNMPv3 protocol, to leverage useful information about the system (without breaking its confidentiality and integrity) [1]. They then collected and analyzed the data to successfully determine the number of devices using SNMP, their vendor and thus potential distribution around the globe. This could be a viable approach for this research, however, instead of running active measurements, we will utilize an already existing dataset.

In this research, all analyzed data will come from a dataset provided by Censys. Censys partners with the private and public sectors to provide the most accurate internet intelligence data available. This allows the network security teams to work with the data and tools necessary to uncover risks and take down threats at scale. Censys builds searchable data sets to support security practitioners in their efforts to make Internet systems more secure and safe. This research will use the data collected on 12th of March 2024 to perform more in-depth analysis of the SNMP-enabled devices. By utilizing the data hidden in the enormous dataset, this work will analyze the number of devices using SNMP protocols in WWW, as well as provide information about the prevalence and distribution of SNMP-enabled devices, including associated vendors and configurations. Additionally, the research will also focus on identifying common vulnerabilities in devices using the SNMP protocol. The final goal of this research will be to determine if there is a difference between the results found in this research, and the results provided in the paper “Third time's not a charm: exploiting SNMPv3 for router fingerprinting”.

2. Problem Statement

When it comes to determining the mapping and distribution of SNMP-enabled devices in the World Wide Web, not enough research has been done. Despite the widespread use of this management protocol, its implementation seems to contain security vulnerabilities that pose risks in practical deployments. Therefore, it is crucial to investigate the current trends of SNMP. This research aims to conduct a detailed analysis of SNMP’s deployment, usage patterns, and associated security vulnerabilities across a variety of devices and services - as cataloged by Censys. By analyzing the dataset, the study will assess the state of security in SNMP-enabled devices and identify prevailing vulnerabilities with the assistance of an API provided by a search engine Shodan. By utilizing the fresh data collected by Censys, valuable data was extracted regarding the evolving landscape of network devices and the latest adoption trends of SNMP. In section 5 there is going to be a comparison between the results of this research and already existing literature.

2.1 Research Questions

The aforementioned problem statement, lead to following research question:

How is SNMP deployed across networks, and what is the latest prevalence and distribution of SNMP-enabled devices on the Internet based on Censys data?

Additionally, those were determined to be suitable sub-research questions that could potentially aid in answering the main research question:

1. What are the prevalence, distribution patterns, and geographical trends of SNMP-enabled devices across different autonomous systems and countries?
2. How can network devices be accurately categorized based on SNMP configurations to identify device types, associated vendors, and potential vulnerabilities?

3. Related Work

To gather related literature and necessary information required for this research, Google Scholar, together with IEEE website was utilized. Search terms such as: “SNMPv3”, “SNMP vulnerabilities”, “Device Fingerprinting” and “SNMP related CVEs” provided a variety of articles and research papers that helped in advancing this research.

Papers analyzing the security and vulnerabilities of SNMP [5], [8], [9], potential enhancements of SNMP security [10] and functionality and performance of SNMP [6] provided valuable insight into how intricate and vast is the world of SNMP-enabled devices. According to source [5], neither SNMPv1 or SNMPv2 provide sufficient security standards to authenticate the source or encrypt the messages exchanged. To counter that SNMPv3 was issued to correct aforementioned deficiencies. This provided insight on how to interpret data regarding SNMP configuration, as according to the source, only version 3 is capable of providing security features to safeguard SNMP-enabled devices. Source [6] stated that the performance of SNMP networks largely depends on the amount of data retrieved. SNMP thrived when a small amount of objects was to be retrieved, but it became apparent that with larger amounts of objects, Web services were more efficient. This information highlighted the role of SNMP for small and medium scale corporations and addressed its limitations that were kept in consideration for this research. Academic studies such as [8], and [9] dwell upon classification and cataloging of the common vulnerabilities found in the devices using SNMP and list a variety of potential solutions and improvements to SNMP, while research of source [10] focused on potential ways to enhance the security of SNMP protocol. All the aforementioned works further motivated the researcher to undertake the analysis of SNMP-enabled devices, especially their security measures based on their configuration and associated vulnerabilities. Special importance goes to two sources [1], [7] that provided great insight into how SNMP measurements can be performed, which parts are to be emphasized, and which are to be omitted.

It is crucial to note that the extent of this research is limited to the amount of data provided in the Censys dataset. While it contains millions of entries from the scans performed on the global network, it still may not guarantee that it contains the entries and addresses of all existing SNMP-enabled devices (due to some devices being available only locally, or simply being on networks that were out of reach during the scans). It is then the combination of the results from different research (mainly [1]), together with this one that may provide new insight into the world of mapping and distribution of devices using SNMP protocol.

4. Methods Of Research

The main method of research was the analysis of particular fields found in the dataset provided by Censys. The size of the whole dataset is around 3 TB and contains almost 2 billion entries in total. It is divided into eight subsets, each containing data collected from different months of late 2023 and early 2024 e.g., subset 1 contains data from measurements performed in August 2023, and subset 8 contains data from scans taken in March 2024. Throughout the analysis period, it was determined that the first four subsets contained almost 10x less data than the later four subsets. Additionally, the first four subsets did not contain any information regarding the configuration of the SNMP agent and its engine specification (engines are service providers that reside in the device and provide services such as sending, receiving, and authenticating messages) i.e., version, boot time, engine time and ID.

Due to the aforementioned limitations of the first four subsets, only 5, 6, 7 and 8 contained sufficient data to accurately answer the RQs stated in the problem statement. Out of the remaining subsets, 7th one did provide very limited information regarding the location and vendor data, and subset 5 and 6 differed very little from the data provided by subset 8. It was then decided that the newest subset, with data collected on March 12th of 2024, would be used, as one of the goals of this research was to update the results of previous works concerning the mapping of active SNMP devices. All collected data was parsed and filtered, to provide insight into the distribution and prevalence of the SNMP-enabled devices over the world.

Additionally, similarly to the research [1], this work analyzed the Engine IDs of each SNMP-enabled device to derive the associated vendors. It was done by extracting bytes 2-4 of the Engine ID to extract OUIs (Organization Unique Identifier), and according to RFC 3411 standard, they were mapped to adequate vendors with the newest version of OUI mapping provided by IEEE (Institute of Electrical and Electronics Engineers). Lastly, the research also focused on determining what are the most common SNMP configurations and what are the potential threats these devices are susceptible to according to the CVE database. The vulnerabilities were determined with the use of the Shodan search engine API, by providing the IPv4 address in the request. Each response returned either a list of CVEs related to the device's IPv4 address, or an empty list if not CVEs were related to that device.

The research was performed with the use of the Python programming language. Python is an open-source, interpreted language that is easy to use and contains a rich collection of libraries with desired functionalities. Since the dataset is large, the research will use one of the available free data-querying engines. In this case Spark was chosen due to a range of benefits, but mainly because it is suitable for real-time processing of large quantities of data over the network. While initially Spark was used for the analysis of the dataset, it quickly turned out that it had performance issues regarding the displaying and manipulation of larger quantities of data within the subsets. Thus Spark data frames would be turned into Pandas data frames, for better optimization. All of the code used for the analysis was executed in a web-based interactive environment called Jupyter Notebook. It allows for easy live code execution and contains tools for visualization of data and results. Libraries such as Numpy, Pandas or Plotly proved to be very useful in managing the dataset, partitioning it, and analyzing and visualizing it.

5. Results

The main questions that this research aims to answer is what is the distribution of SNMP-enabled devices around the world, and how did it change since the measurements performed in 2021. The analysis of the dataset provided insight into the distribution of the most common vendors of SNMP-enabled devices worldwide based on: country, Autonomous Systems, continent as well as information regarding their SNMP configuration and potential vulnerabilities.

5.1 The Available Data

During the research period, it was disclosed that each IPv4 address from the filtered entries appeared uniquely. Additionally, each IPv4 address was not associated with more than one device. This made the analysis much easier to conduct, as each entry was always uniquely linked to only one device.

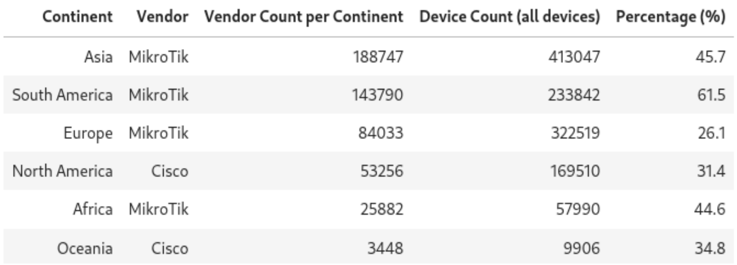
The subset initially contained **246M** row entries, each entry with hundreds of fields with information regarding: different services used by the client i.e., HTTP, SSH or SNMP, the location of the device: continent, country, city, longitude, and latitude, open ports list, DNS, operating system, its version and more. Since this research focuses on SNMP-enabled devices, it was filtered for entries that were related to ports 161 and 162. UDP port 161 connects the SNMP Manager with SNMP Agents, and UDP port 162 is used when the SNMP Agent wants to notify the SNMP Manager about the status of the device or potential issue. After the filtration, there were **20.4M** entries, reducing the subset 10x times. It was then time for analyzing the subset for potentially informative fields regarding SNMP configuration, vendor and software information, the location of the device, the information regarding the Autonomous Systems those devices were connected to, and their IPv4 addresses. The subsets seem to contain IPv4 as the main identifier for the devices since there were only around 2000 entries with valid IPv6 addresses. In total, 13 different columns with information regarding the aforementioned fields were extracted. The research this work is going to be compared to used datasets from two different measurements performed between April 16-20 2021 and April 22-27 2021. They had **31.8M** IP addresses and **18.8M** entries for the engine IDs of the SNMP agents. They have managed to extract **27M** entries with valid IPv4 addresses and valid engine IDs and **12.5M** entries with valid: IPv4s, engine IDs, and engine times (it displays the time in seconds since the device was last rebooted). The subset of the Censys dataset contains around **246M** IPv4 entries, of which only **19.5M** entries are for both valid IPv4 addresses, valid engine IDs and valid IPv4 addresses, valid engine IDs, and valid engine time.

5.2 Deployment & Geographical Distribution of SNMP-Enabled Devices

The analysis had to uncover information regarding the configuration and distribution of SNMP-enabled devices around the world. The research was divided into determining the top 10 vendors for different countries, and Autonomous Systems. Additionally, the analysis provided information about vendor distribution across the continents, and shed light on the market dominance of top vendors around the world.

5.2.1 Vendor Distribution Across Continents.

The previous research determined that the most common vendor on all continents was Cisco. There were in total **134K** devices registered within the EU, **97K** for North America, **81K** for Asia, **22K** for South America, **5K** for Africa, and **5K** for Oceania. In this research, the distribution of vendors per continent looks as follows:



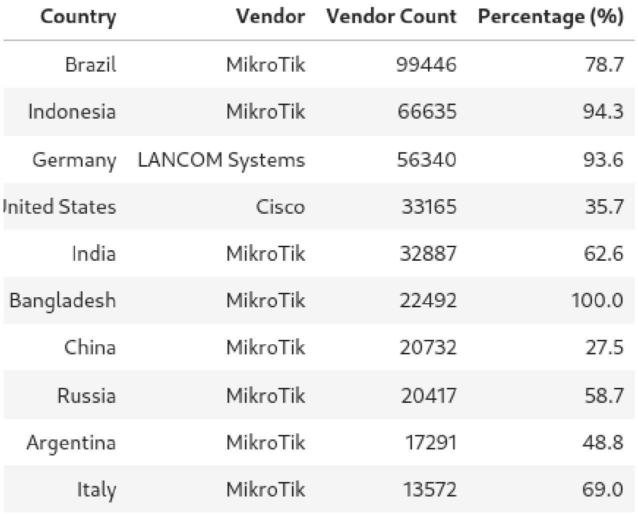
Continent	Vendor	Vendor Count per Continent	Device Count (all devices)	Percentage (%)
Asia	MikroTik	188747	413047	45.7
South America	MikroTik	143790	233842	61.5
Europe	MikroTik	84033	322519	26.1
North America	Cisco	53256	169510	31.4
Africa	MikroTik	25882	57990	44.6
Oceania	Cisco	3448	9906	34.8

Fig. 1. **Table containing top vendors per continent, together with their market share on that continent (in %).**

The results in **Fig. 1**. indicate that Asia was the continent with the biggest concentration of SNMP-enabled devices, according to Censys. What is also interesting is that in the majority of the continents, the top vendor is MikroTik, which was not displayed at all in the previous research. Also, we can see based on the percentage column in **Fig. 1**, the market share of that top vendor in that continent. MikroTik in Asia contains almost half of the market share, in South America it's over half, in Africa it is almost half and in Europe it is only around 1 ⁄ 4. Only North America and Oceania have Cisco as the dominant vendor on the market, with around 30% of the market share. This is an interesting finding, as it shows the dynamic landscape of networking vendors around the world.

5.2.2 Vendor Distribution Across Countries

Nextly, there is the case of top vendors per country. The research this work is being compared to, did not have any information regarding the top vendor per country, however this research does, and it looks as follows:



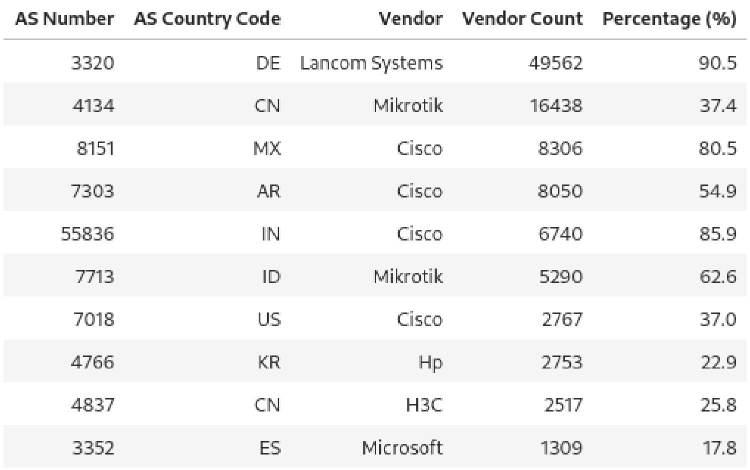
Country	Vendor	Vendor Count	Percentage (%)
Brazil	MikroTik	99446	78.7
Indonesia	MikroTik	66635	94.3
Germany	LANCOM Systems	56340	93.6
Inited States	Cisco	33165	35.7
India	MikroTik	32887	62.6
Bangladesh	MikroTik	22492	100.0
China	MikroTik	20732	27.5
Russia	MikroTik	20417	58.7
Argentina	MikroTik	17291	48.8
Italy	MikroTik	13572	69.0

Fig. 2. Table of most common vendors per top 10 countries with the highest number of SNMP-enabled devices and their market share in that country (in %).

Fig. 2 displays Brazil as the leader, with almost **100K** devices running SNMP protocol. It is interesting to note that almost all of those countries have MikroTik as their top vendor based on market share, and only two have a different top vendor. It can be seen that the vendor dominance in the majority of those countries goes to MikroTik. Nevertheless, it is interesting that in Germany more than 90% of the devices registered with SNMP protocol come from LANCOM Systems.

5.2.3 Vendor Distribution Across Autonomous Systems

Lastly, there is the case of top vendors per Autonomous System While the research “Third time's not a charm: exploiting SNMPv3 for router fingerprinting analyzed the vendor dominance for routers per region for ASes, here the analysis focused on determining the top 10 Autonomous Systems based on the amount of SNMP-enabled devices (with their ASN numbers as identifiers), the country they belong to and what is the top vendor in that AS zone. The result looks as follows:



AS Number	AS Country Code	Vendor	Vendor Count	Percentage (%)
3320	DE	Lancom Systems	49562	90.5
4134	CN	Mikrotik	16438	37.4
8151	MX	Cisco	8306	80.5
7303	AR	Cisco	8050	54.9
55836	IN	Cisco	6740	85.9
7713	ID	Mikrotik	5290	62.6
7018	US	Cisco	2767	37.0
4766	KR	Hp	2753	22.9
4837	CN	H3C	2517	25.8
3352	ES	Microsoft	1309	17.8

Fig. 3. Table of most common vendors per top 10 Autonomous Systems with the number of SNMP-enabled devices per vendor and their market share in that Autonomous System (in %).

It is interesting to note here that according to **Fig. 3** the top place goes to the German Autonomous System with LANCOM Systems as the top vendor. Here the distribution of market share between different vendors is much higher, as we can see vendors such as HP, H3C or Microsoft.

Based on continents, Asia is the one with the highest distribution of such devices and has MikroTik as the vendor with the highest market share of 45.7%. This could relate to the fact that this continent has a population exceeding 4.7 billion people making it a necessity for various IT infrastructures to be efficiently managed.

Based on countries, Brazil is the country with the highest quantity of appliances running SNMP protocol and has again MikroTik as the most common vendor with 78.7% market share. Brazil is one of the largest countries in South America with a population of over 200 million people. This, coupled with significant urbanization, leads to a high demand for networking and communication infrastructure. Still, it would be worth exploring why countries such as China or India are not on the top.

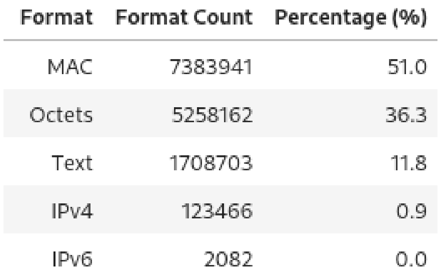
Based on Autonomous Systems, the AS from Germany had the highest number of SNMP-enabled devices and Lancom Systems is the most oftenly used vendor, with 90.5% of market share. Germany has one of the most advanced technological infrastructures and robust IT ecosystems in the world and since the country’s focus is on innovation and technology development, it drives the deployment of numerous SNMP-enabled devices for efficient network management. Here it would be worth investigating why Lancom Systems is the top vendor, and not MikroTik or Cisco.

5.3 SNMP Configurations & Vulnerability Assessment

The sub-research questions were related to the categorization of SNMP-enabled devices based on their configuration and potential vulnerabilities those devices may be susceptible to. Nevertheless, during the early stages of the analysis, it turned out that the subset does contain only a few valuable information regarding the SNMP configuration. The only interesting data that provided insight into potential vulnerabilities such devices might be affected by, was the available versions of the SNMP agent, ID of the engine, the engine time, as well as the vendor of the device and version of the operating system it uses. Thus, this part of the research focused on information that provided insight into the configurations of SNMP-enabled devices and potential vulnerabilities these devices may be susceptible to and their related CVEs.

5.3.1 Distribution of Engine ID Formats

One of the key pieces of information regarding SNMP configuration is the ID of the engine. It's a unique identifier that allows the SNMP managers to easily control the SNMP agent according to their needs. The engine ID can be composed in many different ways, but the most common are based on: the MAC address of the device, its IPv4 address, opaque byte strings called octets, an ASCII representation of some text, or even not SNMP-related (derived by a company based on their algorithm). The distribution of formats looks as follows:



Format	Format Count	Percentage (%)
MAC	7383941	51.0
Octets	5258162	36.3
Text	1708703	11.8
IPv4	123466	0.9
IPv6	2082	0.0

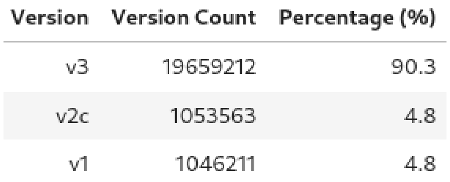
Fig. 4. Table containing the distribution of different engine ID formats of SNMP agents.

It seems that similarly to the research "Third Time's Not a Charm: Exploiting SNMPv3 for Router Fingerprinting", the biggest amount of engine IDs according to **Fig. 4** were composed based on the MAC address of the SNMP agent device. The second most popular option was octets, text-based were third and IDs based on IPv4 addresses were almost last. While the outcome is similar to the one in previous research, there is a discrepancy between the amount of Mac-based engine IDs and Octet-based engine IDs. The research that this work is being compared to, showed that **7.2M** engine ID entries were based on MAC addresses, and only **2.1M** were based on Octets. In this research, **51%** of engine IDs were MAC-based, **36.3**% were octet-based, and **11.8**% were text-based, while in the other one, the ratio was: **58.8**% of engine IDs were MAC-based and only **17**% were Octet based. Additionally, the previous research contained information about engine IDs being composed either through non-SNMP standards or via the Net-SNMP configuration. This research did not contain any information regarding those two options.

5.3.2 Distribution of SNMP Versions

One of the most essential information regarding the SNMP configuration, is the version the agent uses. There are three versions of SNMP: V1, V2C and V3. Versions V1 and V2C are very basic and lack proper security measures. The way users are authenticated is based on a community string (password). "The community string is sent in clear text between the NMS (Network Management System) manager and the agents. Therefore, the managed device is vulnerable to unauthorized users who can easily reconfigure the device, especially if IP access control lists (ACLs) are not in place." [11]. This is a huge security implication, as the password can be easily intercepted if the attacker is on the same network as other SNMP devices via a Man-in-the-middle attack. Version V2C is the successor of version V1, with optimization features regarding the functionality of the protocol. Still, the problems of security and community string have not been properly addressed, so this version is as vulnerable as the first one. Only the third version, V3, actually addressed the security implications. It provides message integrity, authentication, and encryption, as well as prevents message replay and spoofing. The user in the SNMP network must be added to the group, with appropriate levels of authentication and encryption. Only then is the exchange between the agent and the manager possible.

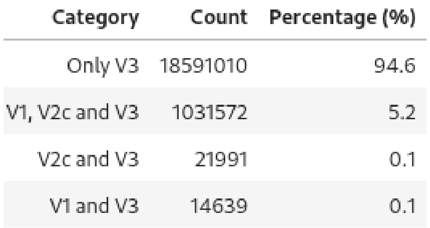
The distribution of used SNMP versions looks as follows:



Version	Version Count	Percentage (%)
v3	19659212	90.3
v2c	1053563	4.8
v1	1046211	4.8

Fig. 5. Table containing the number of devices with different versions of their SNMP configuration in use.

As we can see in **Fig. 5** the vast majority of devices use V3 as the default version for this protocol, which is great news. Only **9.6%** of almost **21M** devices allow for the use of another version, which is still a worrying number as almost **2M** devices are still vulnerable. The research analyzed in more detail the distribution of available versions of SNMP devices. The information looks as follows:



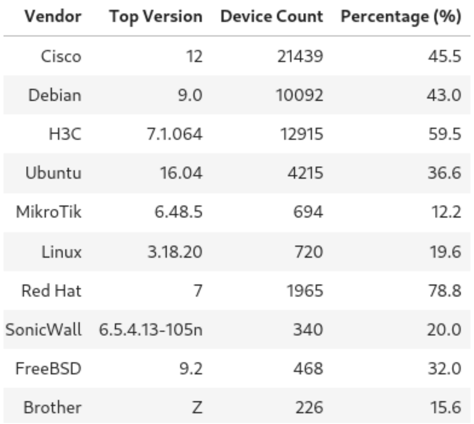
Category	Count	Percentage (%)
Only V3	18591010	94.6
V1, V2c and V3	1031572	5.2
V2c and V3	21991	0.1
V1 and V3	14639	0.1

Fig. 6. Table containing a more detailed number of devices with different versions of their SNMP configuration in use and their equivalent ratio to total number of devices.

It can be seen in **Fig. 6** that every single device has V3 enabled, however, almost **1.05M** devices have other versions configured too. When the V3 is the only active version, then all security implementations are working and cannot be omitted. If the device allows for communication using older versions, then it might end up compromised and susceptible to a wide range of vulnerabilities.

5.3.3 Vendor Analysis

To further advance this research, the analysis also focused on the most common software versions that the SNMP-enabled devices use. This is, after the Engine ID and SNMP version, the most important piece of information that allows the attackers to determine if a device is susceptible to a series of attacks. According to the data available provided by Censys, the top 10 vendors with their most commonly used version look as follows:



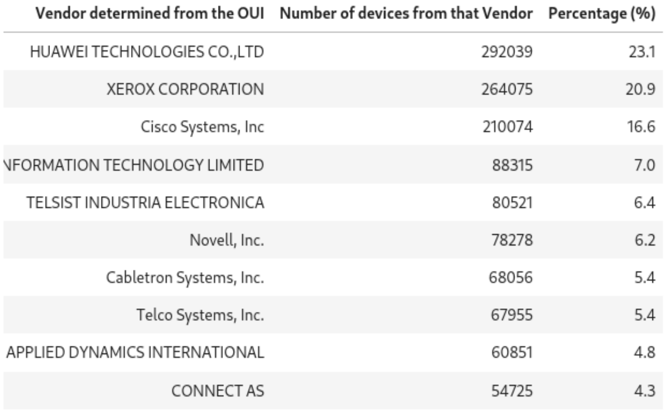
Vendor	Top Version	Device Count	Percentage (%)
Cisco	12	21439	45.5
Debian	9.0	10092	43.0
H3C	7.1.064	12915	59.5
Ubuntu	16.04	4215	36.6
MikroTik	6.48.5	694	12.2
Linux	3.18.20	720	19.6
Red Hat	7	1965	78.8
SonicWall	6.5.4.13-105n	340	20.0
FreeBSD	9.2	468	32.0
Brother	Z	226	15.6

Fig. 7. Table showing the top 10 vendors, their most commonly used software version and the ratio of devices using that version to all devices from that vendor (in %).

Based on available data shown in **Fig. 7** (which was severely limited, as the number of fields with the version of the software were usually empty), we can see that Cisco takes the top spot, with version 12 as the most common one. It is worth mentioning that the current release for Cisco devices is version 15, meaning that the majority of SNMP-enabled devices run outdated software. This increases the chances of attackers compromising the targeted device and using it for a wide variety of malicious practices. MikroTik for example took 5th spot, with version 6.48.5 as the most common. This information, once again, can prove to be very useful to researchers studying the underlying causes of network devices being exploited, but also potential hackers that gain a huge leverage, when determining the version of the software an SNMP agent uses.

5.3.4 Extracted OUIs and Their Associated Vendors

The previous research determined vendors based on their OUI bytes contained within the engine ID of an SNMP agent. While here the vendors were already listed by Censys's scan, it was decided that the research will also contain a brief analysis to determine the top 10 device vendors, based on the OUIs extracted from their engine IDs. The results look as follows:



Vendor determined from the OUI	Number of devices from that Vendor	Percentage (%)
HUAWEI TECHNOLOGIES CO.,LTD	292039	23.1
XEROX CORPORATION	264075	20.9
Cisco Systems, Inc	210074	16.6
NFORMATION TECHNOLOGY LIMITED	88315	7.0
TELSIST INDUSTRIA ELECTRONICA	80521	6.4
Novell, Inc.	78278	6.2
Cabletron Systems, Inc.	68056	5.4
Telco Systems, Inc.	67955	5.4
APPLIED DYNAMICS INTERNATIONAL	60851	4.8
CONNECT AS	54725	4.3

Fig. 8. Top vendors derived from OUIs of the engine IDs and the ratio of this vendor to the total number of devices from all derived vendors (in %).

Comparing the results displayed in **Fig. 8** to the values determined by the research "Third time's not a charm: exploiting SNMPv3 for router fingerprinting" we see some interesting differences. Their top spot was taken by Net-SNMP, second spot went to Cisco, and third went to Broadcom. Net-SNMP is simply a suite of applications used to implement different versions of SNMP using both IPv4 and IPv6 addresses. In this research, the top spot went to Huawei Technologies, with almost **300K** vendor devices determined from extracted OUI bytes from the Engine ID of the agent. In this research, Xerox corporation was second, and Cisco was third. In general, the top vendors from extracted OUI bytes in this research differ greatly from the data collected by the previous research in 2021. This could either imply that: their measurements were taken on a less global scale, unlike Censys which scans all 4 billion possible IPv4 addresses and for each of those scans 100 most commonly used ports, or there was a shift in vendor market dominance. In both cases, the result shed light on the distribution of top vendors based on the OUIs extracted from the Engine ID, which provided useful information regarding the distribution of SNMP configurations.

Based on the gathered data, the SNMP-enabled devices could be categorized based on the combination of the SNMP version they use and the OUIs extracted from Engine IDs. If the only version used by the device is V3, then we can safely assume that it is more secure than if it is using any earlier version of SNMP (as shown in **Fig. 6.**). Additionally, by extracting the OUIs from the Engine ID and using the mapping provided by IEEE institute, the research determined a particular vendor of the device, which could aid in categorizing the type of the device for future research.

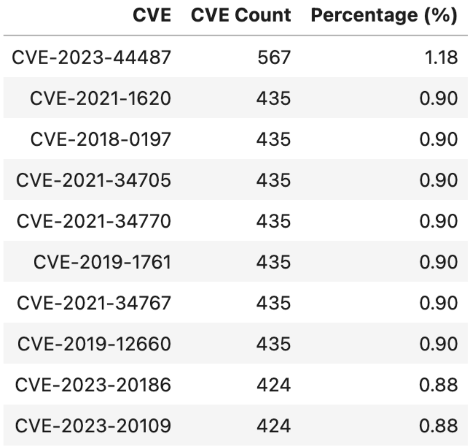
5.3.5 Vulnerability Assessment of SNMP Devices

Lastly, the final goal of this part of the analysis was to determine the common vulnerabilities those systems may contain due to incorrect SNMP configuration. While the information that the research collected so far would be enough to manually determine the potential vulnerabilities based on the CVE database, another, more automated approach was chosen. The analysis utilized the API of a cybersecurity-related search engine called "Shodan". The search engine allows for discovering the network devices on the internet based on different protocols. The link to the used API looks as follows:

https://internetdb.shodan.io/{ip}

The **{ip}** variable is an IPv4 address in the form of four octets. In section 5 it was mentioned that each device in the dataset is unique, and that each IPv4 address only belongs to one device in the dataset. While this helped a lot, it was not possible to determine the list of vulnerabilities for all **21M** devices in the subset, as for each IP address, a request would have to be sent to Shodan's API and a response would have to be processed. Due to that it was decided that the data would be collected only for **10K** devices, which already took a substantial time to collect.

Now, to answer the final sub-research question, out of all determined vulnerabilities for **10K** devices, the investigated vulnerabilities that most consistently appeared in relation to SNMP-enabled devices were:



CVE	CVE Count	Percentage (%)
CVE-2023-44487	567	1.18
CVE-2021-1620	435	0.90
CVE-2018-0197	435	0.90
CVE-2021-34705	435	0.90
CVE-2021-34770	435	0.90
CVE-2019-1761	435	0.90
CVE-2021-34767	435	0.90
CVE-2019-12660	435	0.90
CVE-2023-20186	424	0.88
CVE-2023-20109	424	0.88

Fig. 9. Most common vulnerabilities related to SNMP-enabled devices and the ratio of this CVE to the total number of extracted CVEs (in %).

Out of 10K requests, only **1338** returned lists of available vulnerabilities (remaining 8762 returned an empty list). In total the research determined **1427 unique** CVEs related to those 1338 devices and **46976** CVEs **in total** for all devices that returned a non-empty list. The ratio of a particular CVE to the total number of determined CVEs varied between **0%** and **1.18%**. The difference between those was not significant enough, thus **Fig. 9** displays only CVEs with the count value of more than **400** to emphasize their significance

CVE-2023-44487 is linked to the HTTP/2 protocol and does not relate to a specific vendor. The CVE describes how it is possible to perform denial of service attacks, due to the malfunction of too quick request cancellation, resulting in flooding of the server with data. (**CVE risk - High**)

CVE-2021-1620 is linked to Cisco IOS and Internet Key Exchange (IKEv2), which could allow authenticated remote attackers to exhaust the free IP addresses from the assigned local pool, which would prevent users from logging in and would lead to Denial of Service attack. (**CVE risk - High**)

CVE-2018-0197 relates to Cisco IOS Software and allows for an unauthenticated attacker to cause a denial of service attack by corrupting the VLAN Trunking Protocol database. (**CVE risk - Medium**)

CVE-2021-34705 is related to multiple vulnerabilities in the administrative web-based GUI configuration manager of Cisco Firepower Management Center (FMC). Those would allow authenticated remote attackers to access sensitive configuration information. (**CVE risk - Medium**)

CVE-2021-34770 is linked to Cisco IOS XE Software for Cisco Catalyst 9000 Family Wireless Controllers. The vulnerability occurs due to a logic error during the validation of CAPWAP (Control and Provisioning of Wireless Access Points) packets. With this exploit, the device could allow an unauthenticated, remote attacker to execute arbitrary code with administrative privileges or cause a denial of service attack by crashing the device. (**CVE risk - Critical**)

CVE-2019-1761 relates to Cisco IOS software and the Host Standby Router Protocol (HSRP) and allows an unauthenticated attacker to receive potentially sensitive information from an affected device. (**CVE risk - Medium**)

CVE-2018-12660 relates to Cisco IOS Software, allowing an authenticated local attacker to alter the memory of an affected device. A successful exploit provides the attacker with the ability to modify the configuration of the device. (**CVE risk - Medium**)

CVE-2021-34767 relates to Cisco IOS Software for Cisco Catalyst 9000 Family Wireless Controllers. This vulnerability leads to a denial of service attack for a specific VLAN within the configured network. By sending a specially crafted IPv6 packet via a wired networking interface to a vulnerable device, an attacker could successfully trigger a Denial of Service attack by causing traffic stops in the affected VLAN. (**CVE risk - High**)

CVE-2023-20109 is related to Cisco IOS and a Cisco Group Encrypted Transport VPN. The vulnerability could allow an authenticated remote attacker who has administrative control of a group member or a key server to execute arbitrary code on an affected device. (**CVE risk - Medium**)

CVE-2023-20186 relates to Cisco IOS Software and the Authentication, Authorization and Accounting feature (AAA). The vulnerability could allow an authenticated remote attacker to bypass authorization and copy files from and to the file system of an affected device using Secure Copy Protocol (SCP) (**CVE risk - High**)

Four out of ten of the aforementioned vulnerabilities are related to Denial of Service attacks, which may cause disruptions in the workflow of a network with SNMP-enabled clients. Four out of ten vulnerabilities are related to extraction of the data from and to affected devices or manipulating device's configuration, providing the attacker with countless opportunities to use the device as the entry point further into the network, execute various scans and exploits on this or other devices on the networks, or exfiltrate confidential data. The remaining two are the most dangerous, as they allow the attacker to execute arbitrary code with administrative privileges, giving the full control of that device to them. The distribution of such attacks is not random, as those four types, if exploited, could be disastrous for companies that require many different types of devices to work harmoniously. It is also interesting to note that a vast majority of those exploits are related to Cisco software running Ftop on IOS devices, flagging the importance of company awareness and regular updates against such vulnerabilities.

7. Limitations and Future Work

One of the main limitations was the size of the dataset. Its size is around 3 TB, and the only way to access the data was via SSH. Due to a large number of entries to analyze, the first major obstacle was to determine which fields are useful for this research, as there were more than a hundred individual fields related to various services, open ports lists, locations, ASs, etc. While the dataset is divided into 8 subsets, the first four do not contain nearly enough information to be useful in comparison with the results of the research: "Third time's not a charm: exploiting SNMPv3 for router fingerprinting". Another issue was the usage of the spark framework. While it was very versatile, it halted the research in the early stages, as it would constantly produce various errors that would force the user to reload the kernel of Jupyter Notebook, making the analysis very tiresome and time-consuming. The only way to overcome this issue was to choose particular fields that the researcher would like to extract from the subset and turn those into a Pandas data frame. Pandas data frames were much faster in loading, displaying, and manipulating available data, eradicating all of the problems that were linked to Spark. Lastly, there was the case of analyzing the potential vulnerabilities of devices based on their IPv4 address. Since the analysis had to use the Shodan API, there could only be a limited amount of requests that could be made, before the security features of that website would (presumably) temporarily block the research device from sending more requests. There were efforts to ensure that the vulnerability lists are retrieved for 10K unique devices, but unfortunately it was not possible due to the aforementioned behavior of the API. Thus, the part of the research regarding the top vulnerabilities was only shown for only 1338 devices, out of almost **20M** available for analysis. There was no way of improving the implementation, as the only way would be to modify the API request to be less frequent, which would exponentially increase the waiting time for the results.

This research still contains information that could be gathered and analyzed for future use regarding networking devices, their distribution, and prevalence. Censys did a fantastic job at collecting and organizing information regarding SNMP-enabled devices around the globe, but it also contains information about so many other services and more. With the proper amount of time, lots of useful information could be gathered that would provide more insight regarding the distribution and prevalence of various services other than SNMP. Another solution would be to train a Machine Learning model using those datasets to discover more insights, but such a task is very time-consuming and may not yield any improvements when it comes to the analysis. Lastly, it would be reasonable to perform separate research focused on analyzing investigated CVEs, automating the CVE extraction method, and optimizing it in order to be able to send more than 10K requests. If this research is ever continued, the employment of a ML algorithm could prove to be very efficient and time-saving for the researcher.

8. Discussion

First, it can be noticed that there was a sizable shift between the top vendors and their market dominance worldwide. The research this work is being compared to, had its data collected in 2021, where the major vendor was Cisco. It took less than 3 years for this dominance to shrink and be given to another - MikroTik. It can be speculated that this shift was mainly due to the competitive features and prices provided by MikroTik. Cisco vendors are still prevalent in North America, parts of Africa, and the majority of Oceania. On the other hand, almost the entire Asia, South America, and Europe have MikroTik as their most common vendor.

Second, this research has updated the knowledge regarding the distribution of SNMP devices around the world per continent, country, and autonomous systems. Asia was the continent with the largest number of SNMP devices, mainly by having the highest population out of any other continent. Then countries: Brazil, USA, China, Germany, Russia, India, and Indonesia were in the top 6 with the largest number of SNMP devices, mainly due to the high population and highly developed IT systems in those areas. Lastly, autonomous systems with ASNs: 3320 in Germany, 4134 in China, and 8151 in Mexico, were the top 3 autonomous systems with the largest number of SNMP-enabled devices connected to them. This is more interesting, as it seems that those three AS were located in areas with the highest concentration of IT systems, with Germany being the top 1.

It was also determined that the vast majority of the appliances in this subset use only V3 as the version for any form of communication between the SNMP manager and SNMP agents. This is very reassuring, as only the third version provides proper security standards, meaning that many IT administrators adhere to proper security standards.

Another element of SNMP configuration analyzed was the engine ID of the SNMP agent. Based on the OUI bytes extracted from this ID,, the research determined that the top 3 vendors that use SNMP protocol are: Huawei Technologies, Xerox Corporations, and Cisco Systems.

Lastly, with the help of a search engine called Shodan, and their API, this analysis was able to determine the vulnerabilities that these appliances may be susceptible to. The top 10 most common vulnerabilities associated with appliances using this protocol were CVEs regarding:

- Denial of Service: **CVE-2023-4487, CVE-2018-0197, CVE-2021-1620, CVE-2021-34767**
- Data Extraction: **CVE-2023-20186, CVE-2021-34750, CVE-2019-1761**.
- Configuration Manipulation: **CVE-2018-12660**
- Remote Code Execution: **CVE-2023-20109, CVE-2021-34770.**

Majority was related to IOS software, creating questions regarding the state of security in Apple devices.

9. Conclusion

This research analyzed the geographical distribution and vendor dominance of SNMP-enabled devices across: continents, countries and Autonomous Systems. It shed light on the common configurations of SNMP devices based on Engine IDs and versions, as well as, determined most common vulnerabilities that these devices may be susceptible to.

The results of this analysis provide insight on the dynamic landscape of SNMP-enabled devices, either by comparing the results to the ones from the research "Third time's not a charm: exploiting SNMPv3 for router fingerprinting", or determining new information not disclosed in the aforementioned paper. The results also update the information regarding vendor distribution across three different categories (country, continent, AS) that were lastly determined in 2021. The research showed that the information stored in Engine IDs of SNMP configurations may be utilized to successfully fingerprint associated vendors and that a lot of devices running SNMP protocol are susceptible to various vulnerabilities.

The implications of the last part of the results regarding common exploits could be useful in increasing the awareness and security of SNMP-devices. The results prove how crucial it is to: perform regular updates, ensure only one version is in active use and that there is something/someone that actively and frequently monitors them. It is difficult to determine what the landscape of SNMP-enabled devices will look like in the future, but based on how dynamic it is, it for sure will be the subject of another analysis.

10. Use of chat GPT

During this research, the author used chatGPT to: occasionally ask questions regarding particular code execution issues. After using this tool, the author reviewed and edited the content as needed and takes full responsibility for the content of the work.

11. References

[1] Albakour, T., Gasser, O., Beverly, R., & Smaragdakis, G. (2021, November). Third time's not a charm: exploiting SNMPv3 for router fingerprinting. In *Proceedings of the 21st ACM Internet Measurement Conference* (pp. 150-164).

[2] TTRO.com. (n.d.). 5.1 uses of networks. *Siyavula*. Retrieved May 4, 2024, from https://www.siyavula.com/read/za/information-technology/grade-10/networks/05-networks

[3] Mauro, D., & Schmidt, K. (2005). *Essential SNMP: Help for System and Network Administrators*. " O'Reilly Media, Inc.".

[4] Taylor, P. (2023, June 23). Connected Devices Worldwide 2014-2028. *Statista*. Retrieved May 4, 2024, from https://www.statista.com/statistics/512650/worldwide-connected -devices-amount/

[5] Stallings, W. (1998). Security comes to SNMP: the new SNMPv3 proposed internet standards. *The Internet Protocol Journal*, *1*(3), 1-12.

[6] Pras, A., Drevers, T., van de Meent, R., & Quartel, D. (2004). Comparing the performance of SNMP and web services-based management. *IEEE Transactions on Network and Service Management*, *1*(2), 72-82.

[7] Schonwalder, J., Pras, A., Harvan, M., Schippers, J., & van de Meent, R. (2007, May). SNMP traffic analysis: approaches, tools, and first results. In *2007 10th IFIP/IEEE International Symposium on Integrated Network Management* (pp. 323-332). IEEE.

[8] Jiang, G. (2002). Multiple vulnerabilities in SNMP. *Computer*, *35*(4), supl2-supl4.

[9] Singh, A., Singh, B., & Joseph, H. (2008). Vulnerability Analysis for SNMP and LDAP. In *Vulnerability Analysis and Defense for the Internet* (pp. 125-134). Boston, MA: Springer US.

[10] Otrok, H., Mourad, A., Debbabi, M., & Assi, C. (2005, June). Improving the security of SNMP in wireless networks. In *2005 International Conference on Wireless Networks, Communications and Mobile Computing* (Vol. 1, pp. 198-202). IEEE.

[11] Noction. (2023b, March 14). SNMP evolution and version differences. SNMP security models/levels details. Noction.
https://www.noction.com/blog/snmp-versions-evolution-security