White Paper

Bitdefender®

The IoT Threat Landscape and Top Smart Home Vulnerabilities in 2018

Author: Luana Pascu

Introduction

The IoT market has been booming in the past two years, impacting both consumers and businesses across sectors worldwide. Even though the technology has been widely adopted with great enthusiasm, a thorough security pattern still hasn't been properly discussed to ensure its further growth in an increasingly sophisticated threat landscape.

Following large-scale cyberattacks launched through exploited IoT botnets in the past two years, IoT risk awareness has slightly increased, yet smart devices are still vulnerable. One major cause is that manufacturers rush to deliver innovative gadgets that catch the eye of the consumer, but completely disregard end-to-end encryption.

Many smart devices currently available on the market are vulnerable to third-party intrusions. Because traditional security software can't fend off attacks, home and enterprise networks are left defenseless. The industry is not far from jeopardizing users' physical safety, as vulnerabilities have been detected on multiple occasions in medical devices, pacemakers, security cameras, smart doorbells, baby monitors and connected cars.

Ideally, two solutions to the problem would be to integrate security from the design stage, and to enforce a security and risk management pattern issued as a joint effort of legislators, security experts and manufacturers. IoT security is approached with uncertainty as tech leaders have trouble defining accurate guidelines for overall deployment. While the industry struggles with risk management, hackers surely don't waste their time in taking advantage of the lack of a unified security approach and technical standards to develop complex attack strategies to bypass traditional security.

It is impossible to apply classical security solutions to smart devices such as smart TVs, connected home appliances, wearables, smart entertainment or connected cars, so an integrated approach to security is paramount. An accessible temporary fix would be an increase in security awareness among consumers.

How Security Aware are Smart Home Owners?

The average smart home is filled with connected devices such as gaming consoles, baby monitors, smart TVs and wireless surveillance systems. What users don't know is that a worryingly high proportion of IoT device are sold without in-built security and even lack an operating system that supports the installation of security software agents.

The Internet of Things market is growing exponentially, with 20.8 billion connected devices forecast to be in use globally by 2020, according to Gartner. IoT value is increasing, and so are budgets allocated for this technology. IDC expects that, by 2019, investments will near $1.3 trillion, compared with $591.7 billion in 2014, at a compound annual growth rate of 17%.

The rise of machine-to-machine communication and the surge in consumer smartphone usage, Internet, and social networks have established IoT security as a strategic pillar in the digital landscape. Users should look into deploying a complete, multilayered cybersecurity solution that immediately pinpoints weaknesses in infrastructure and prevent snoops from hijacking smart devices. A solution based on advanced machine learning algorithms that leverages years of experience in vulnerability assessment and detection could reduce risks.

No smart device is insignificant, as each represents a potential attack avenue hackers can manipulate to get inside a home network and take control over all devices linked to it. The average smart home in the United States houses 11 smart devices, including accessories, at a common rate of 2 devices per home, according to a Bitdefender study. The most common smart devices in US homes are smartphones (91%), smart TVs (73%) and tablets (72%).

Weak usernames and passwords, negligent browsing, as well as the lack of firmware updates aid hackers in getting access to banking information, private photos and videos, e-mails, home security settings and eavesdropping through baby monitors and smart TVs. **58% of owners** use **different passwords** for **each smart device** and **24%** have several **passwords they use randomly**.

Every day, consumers expose themselves to phishing and fraud risks by accessing suspicious and malicious URLs or by not ensuring the website they access are HTTPS. Most often, users don't even bother checking for updates for their routers or smart devices. **Four out of 10 smart device users in the US updated** their **wireless router in 2017 and 65% ran firmware updates** (vs. **39%** - total).

Key Facts

- **5 out of 10 smart TV** users **haven't updated** the software apps on their devices **in over a month**.
- **6 out of 10 users did not** perform any **firmware** updates on their **wireless router throughout its lifespan.**
- **38% of smartphone and tablet users** did **not run a firmware update**
- **55% of smart TV users** did not run a firmware update
- **Only 6 out of 10 smart device users** say they have **different passwords for each smart device**/ accessory.
- **2 out of 10** have several passwords that they **randomly use**.
- **1 out of 10** use **one password** for all their smart devices
- **7 out of 10 smartphone** or **tablet** users say that they changed the passwords on these devices **more than 3 months ago**.
- Also, **5 out of 10** of **smart TV** owners said that they **have never changed** the password on their device.

Identity Theft and Data Leaks among Top Concerns for US Smart Device Owners

Due to an increasing number of unencrypted connections and vulnerability exploits in the wild, login credentials are often leaked. As a result, personal data is no longer kept private. Tremendous amounts of data are shared every second on social media – videos, photos, likes and opinions – information that could be exploited if not secured.

Smart devices collect data in real time and send it to manufacturers on the grounds that it optimizes user experience. Bitdefender research shows 61% of smart device users keep their information on their personal computer or laptop, while 68% of the age segment 18 – 22 specifically keep their personal information on their phones.

Even though smart device owners keep valuable data on their devices, they are concerned that their identity could be stolen (58%), that sensitive information can be exfiltrated at any time (56%) and that the devices can get infected with malware (55%). Since only 1 out of 10 users has no concerns about the security of their smart devices, it means they are slightly more educated about online security and risks than in previous years.

Key Facts

- **6 out of 10** users are concerned their identity could be stolen**,** that **sensitive information can be accessed** or that **their devices can get infected with malware.**
- **7 out of 10** users have **at least one camera** connected to the Internet through a vulnerable router**.**
- **3 out of 10** users of smart devices are concerned that **someone could gain access to the device camera** and that they can be **recorded without their knowledge**.
- **Only 11% of the users** keep their information and documents **on dedicated storage solutions attached to their home network (NAS).**
- **61%** of them keep the private files and documents on their **personal computer/ laptop**.
- **50%** store the personal information on their **phones**.

BOX Telemetry

Foreword

The IoT space has exploded over the past three years as the smart home has become increasingly interconnected. Apart from forecasts and studies, the composition of the smart home remains widely unknown.

Bitdefender, the creator of the world's first security solution for the smart home, is continuously monitoring this space. This whitepaper aims at painting a relevant picture of the device prevalence inside the smart home and offers insight into the vulnerabilities affecting consumer-grade IoT devices.

A reduced price in sensors combined with cheaper gadgets and extensive media promotion has turned home automation into a hot trend. A hot trend that, nevertheless, opens up new attack vectors for hackers. Sure, consumers are excited that in the near future machines can take over everyday operations such as scanning the fridge for expired food, analyzing their health based on statistics collected by wearables, turning devices on and off, and controlling heating, lighting and home alarm systems. People have been dreaming about this type of innovation since the popular 1960s show The Jetsons - no wonder the demand for smart devices has increased in the past years.

Gartner predicts IoT budgets will surpass EUR 1 billion in 2018, but what does this exactly mean for security? According to the same research, there is now more awareness about the IoT threat landscape and risks posed by vulnerabilities, hence the budget increase. Mindful of popular demand for connected devices, cybercriminals are deviating from their traditional attack methods by developing new strategies based on easily exploitable smart devices. The main roadblock to the widespread adoption of IoT is security, and the more users understand its critical importance and clearly demand it, the more manufacturers will shift their focus from simply releasing vulnerable devices to creating innovative smart devices with top-notch security.

The issue with IoT devices is twofold. On one hand, the average, non-technical IoT buyer has little to no knowledge of their inner workings. Nor do they have the necessary networking skills to firewall potentially open ports.

On the other hand, the setup process itself is rarely optimized for security. Sometimes, the setup process does not force the user to choose a customized, hard-to guess password for administrative accounts on the device.

Automated attacks that rely on IP and port scanning are the new normal. Different size botnets come and go daily as they ceaselessly get hijacked by competing bot operators, and customers and the security industry alike have no visibility into this space.

A look inside the smart home

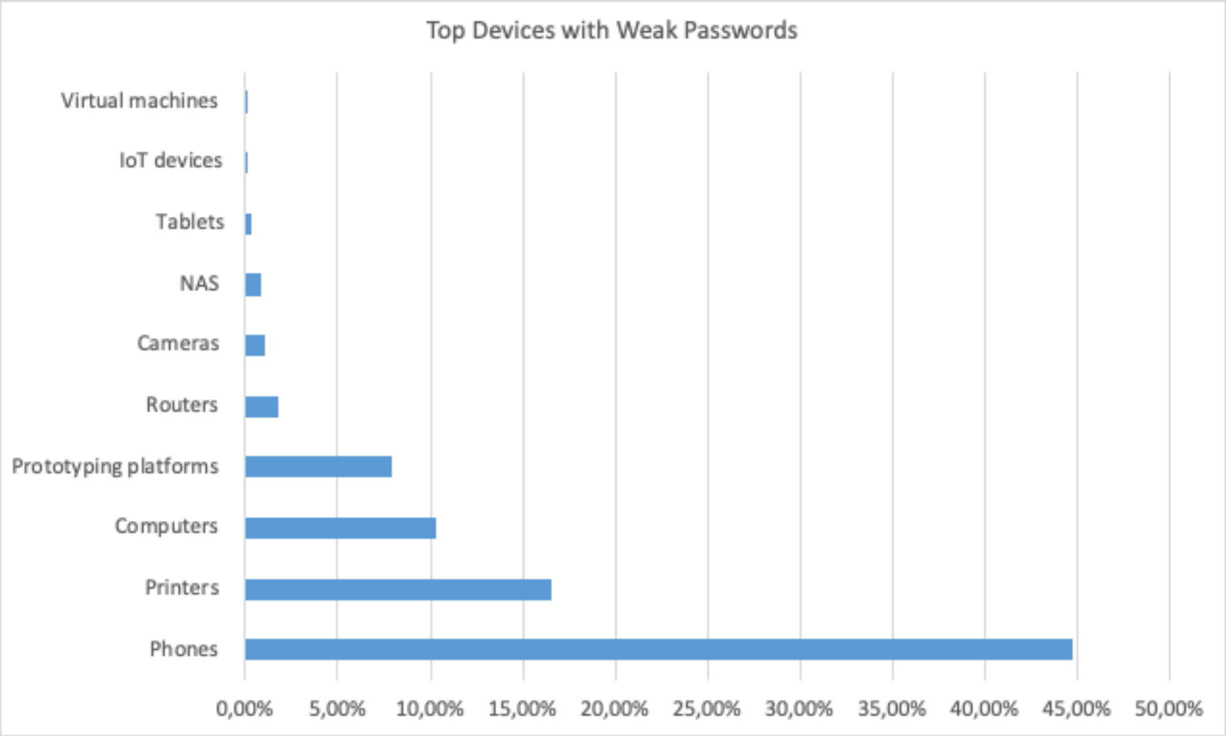
On average, the regular smart home ecosystem is comprised of **20 smart devices**, including the household gateway or router. The Vulnerability Assesment technology developed by Bitdefender reveals that 95 percent of the vulnerabilities detected in the smart home reside in the firmware. Over 9,000 of the identified vulnerabilities had already been made public, which means that exploitation proof of concept code is already available to be used against victims.

Vulnerability breakdown in the smart home

5% of all internet-connected devices ran on weak passwords, representing either hidden or vendor backdoors, as well as weak login passwords on web interfaces that users forgot or ignored.

Security experts advise users to update their passwords and ensure they are unique and complex, but this instruction is most often ignored. According to telemetry collected from Bitdefender BOX units, 50% of printers have the weakest passwords in a smart home, but only 5% of IP cameras were found with weak passwords. NAS (Network attached storage) devices have better, more complex passwords, as only 0.2% were found vulnerable due to poor passwords.

The weakest passwords were overall detected in phones (44.78%), printers (16.60%), and computers (10.32%), while stronger passwords were found securing prototyping platforms (7.97%), routers (1.79%), cameras (1.05%), NAS (0.83%), tablets (0.29%) and IoT devices (0.16%).

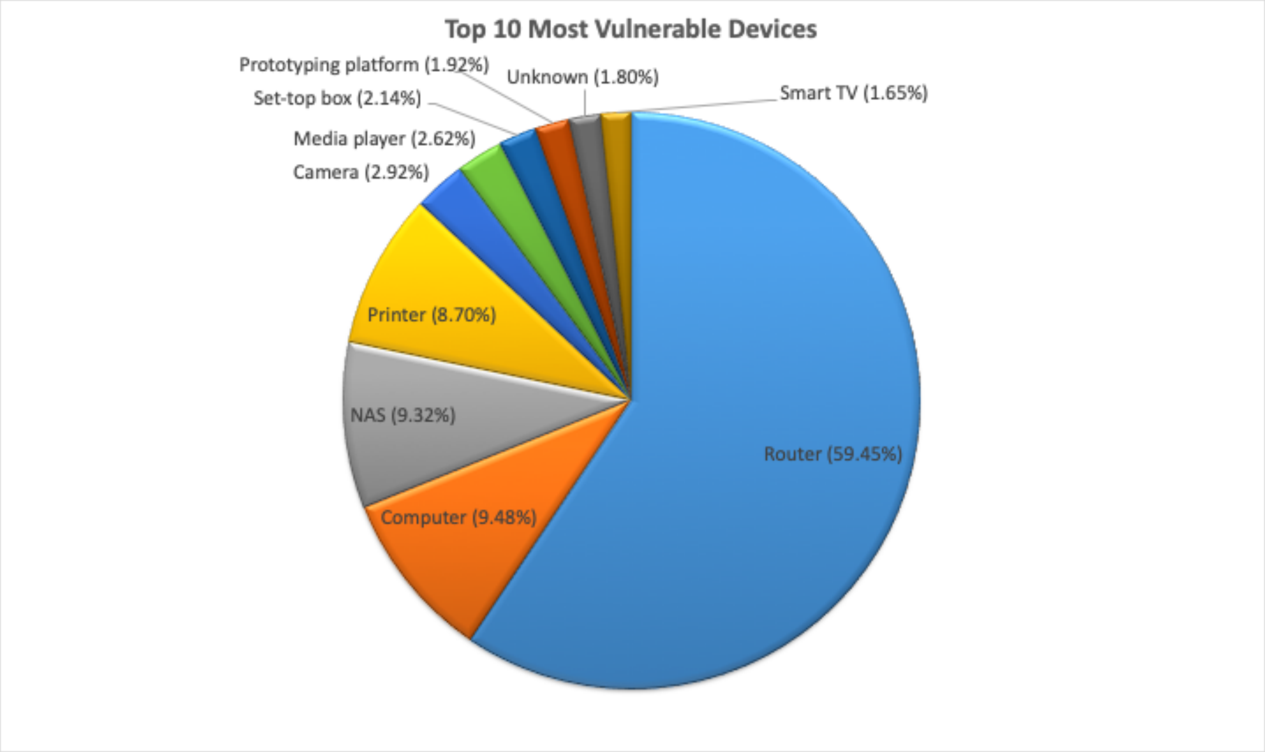


In 30 days, Bitdefender BOX blocked 461,718 threats, out of which 75.97% were web-based (dangerous websites). Of the total number of vulnerabilities identified, 95% are common vulnerabilities and exposures (CVE). In most cases, a device with vulnerable firmware comes with multiple other vulnerabilities.

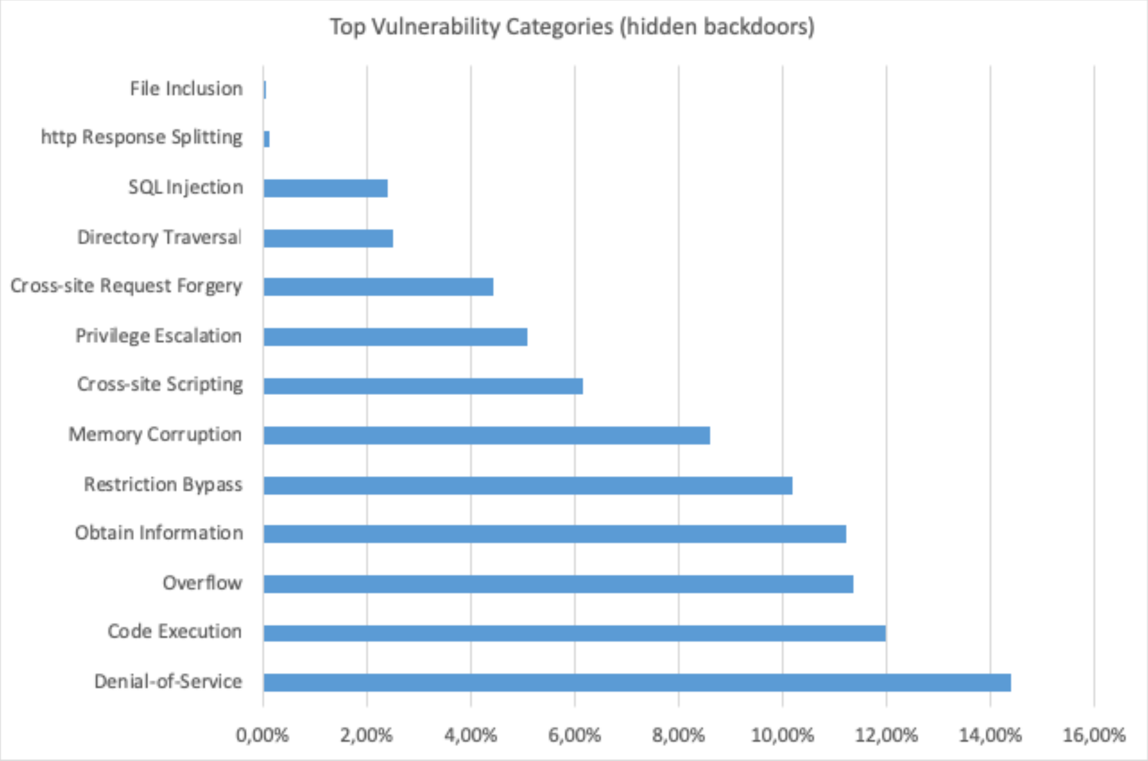
The top common vulnerabilities and exposures identified are Denial-of-Service (42%), Overflow (21%), Code Execution (10%), Obtain Information (7%), Bypass Restriction (3.8%), and Memory Corruption (3.4%).

The main types of attack blocked by Bitdefender BOX are Untrusted URL (64%), Phishing URL (25.8%), Unencrypted Private Data (15.4%), Malware URL (8.5%) and Fraud URL (1.5%).

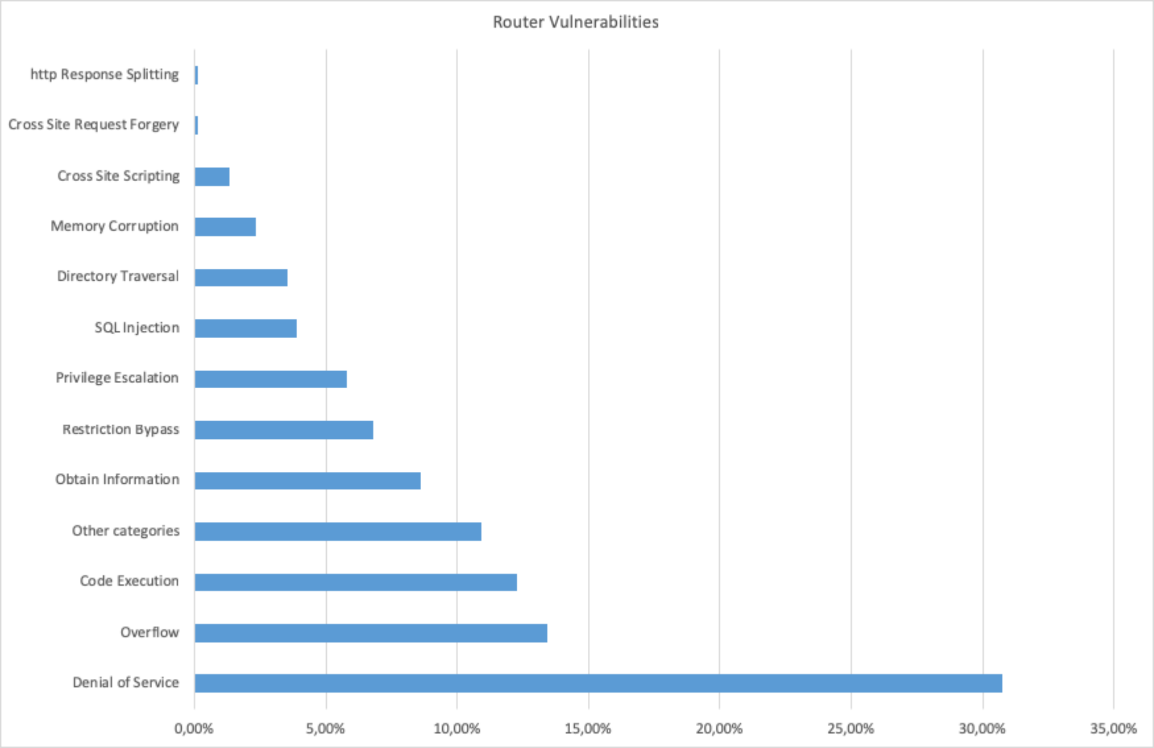
The most vulnerable internet-connected devices are routers (59.45%), followed by computers (9.48%), NAS (9.32%), printers (8.70%), cameras (2.92%), media players (2.62%), set-top boxes (2.14%), prototyping platforms (1.92%) and smart TVs (1.65%).



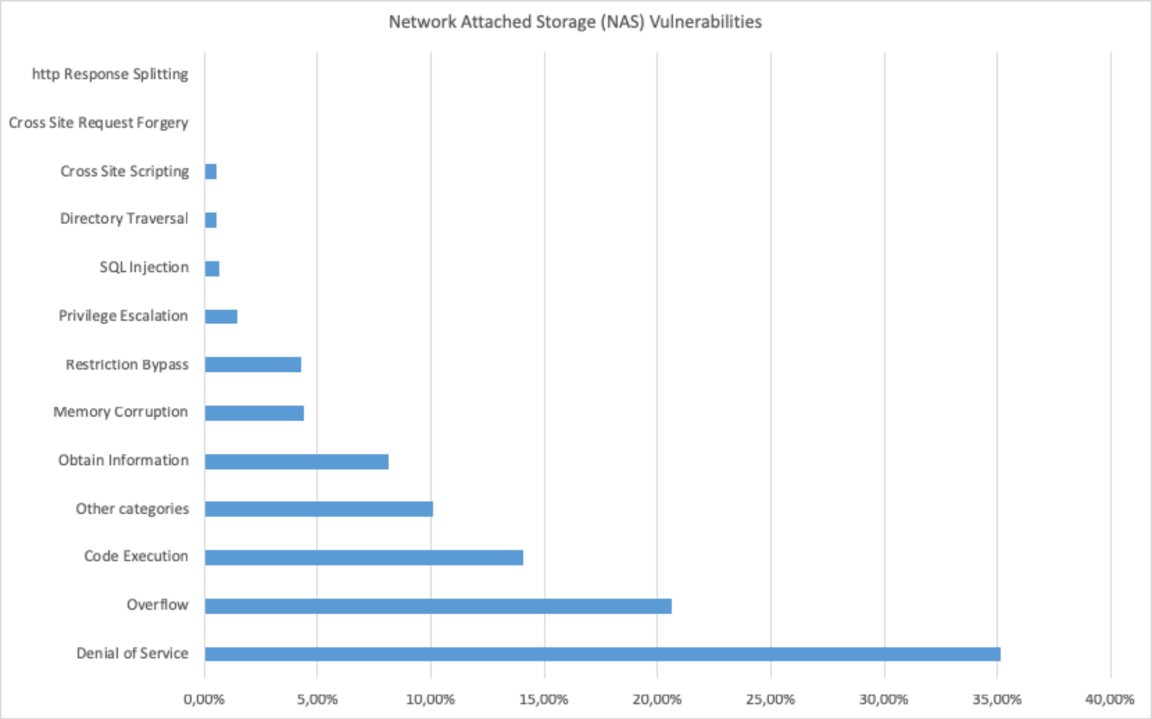
According to Bitdefender telemetry, the majority of attacks on smart devices in 2017 originated from Denial-of-Service vulnerabilities (14.39%), Code Execution (11.99%), Overflow (11.35%), Obtain Information (11.22%), Restriction Bypass (10.17%), Memory Corruption (8.60%), Cross-Site Scripting (6.14%), Privilege Escalation (5.09%), Cross-Site Request Forgery (4.42%), Directory Traversal (2.50%), SQL Injection (2.38%), http Response Splitting (0.13%) and File Inclusion (0.03%).



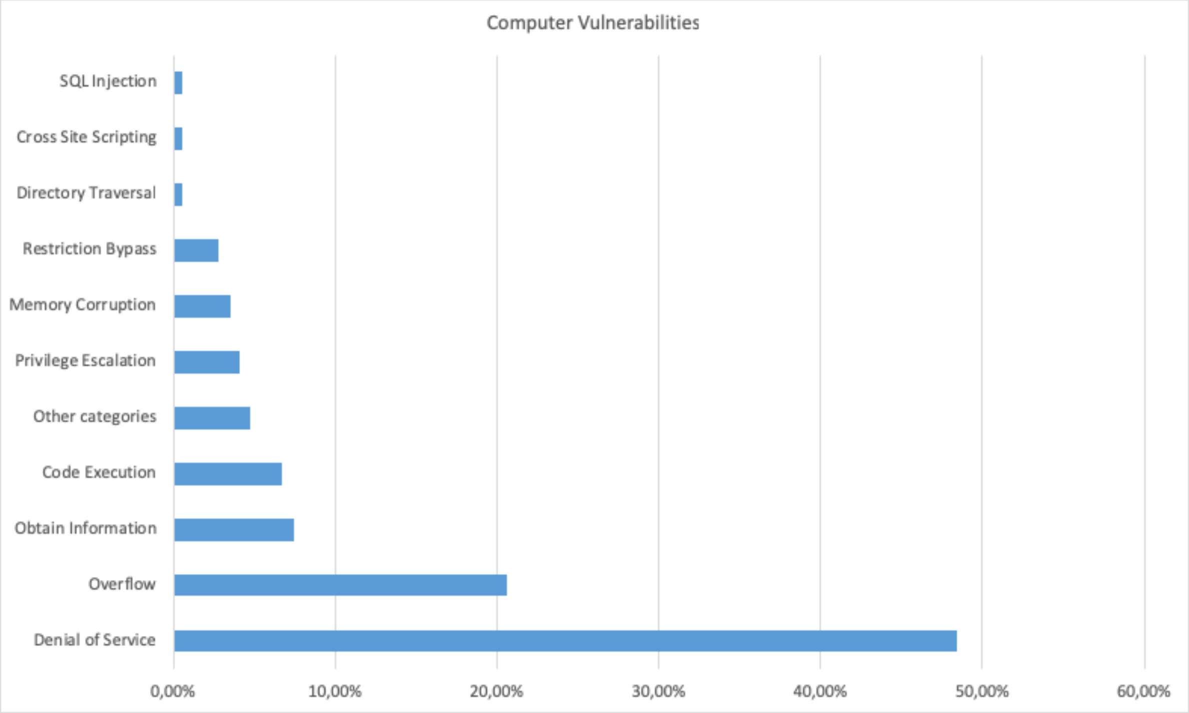
The most common vulnerabilities detected on **routers** are Denial-of-Service (30.75%), Overflow (13.43%), Code Execution (12.30%), Obtain Information (8.61%), Restriction Bypass (6.82%), Privilege Escalation (5.82%), SQL Injection (3.91%), Directory Traversal (3.56%), Memory Corruption (2.32%), Cross-Site Scripting (1.33%), Cross-Site Request Forgery (0.13%) and http Response Splitting (0.13%).



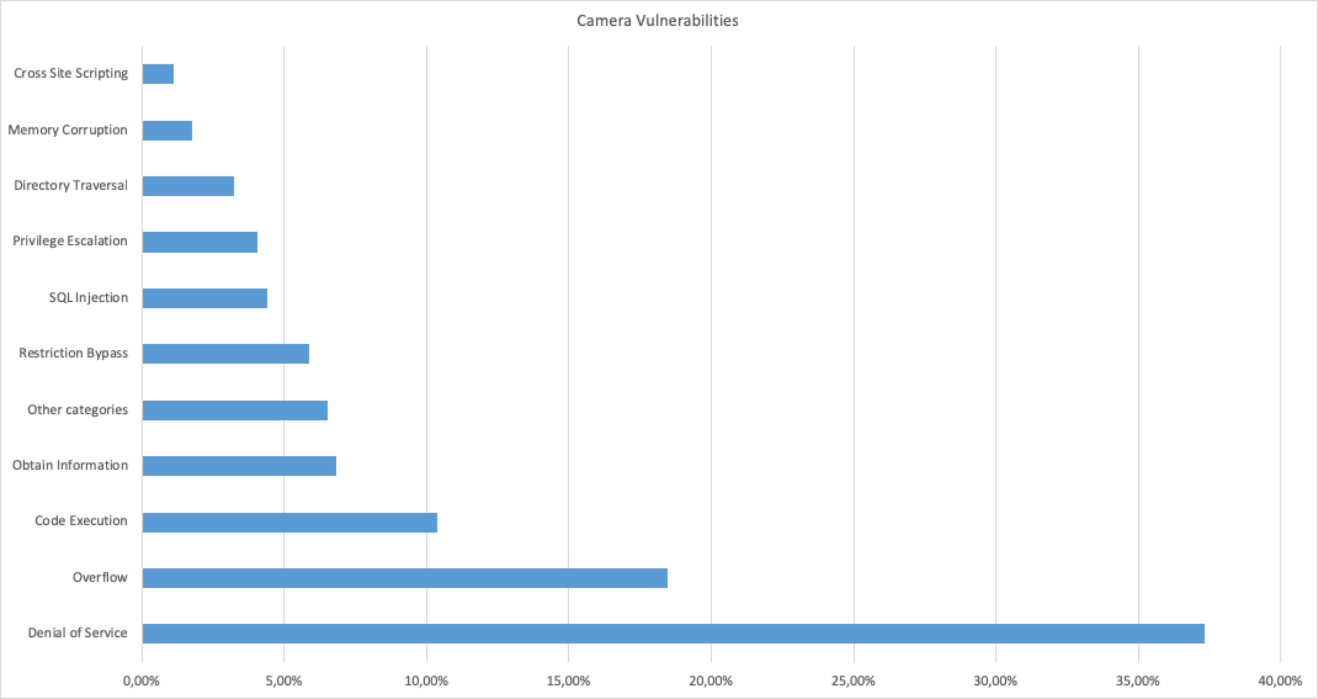
The **top vulnerabilities** detected on **Network attached storage (NAS)** are Denial-of-Service (35.12%), Overflow (20.60%), Code Execution (14.08%), Obtain Information (8.13%), Memory Corruption (4.40%), Restriction Bypass (4.29%), Privilege Escalation (1.48%), SQL Injection (0.66%), Directory Traversal (0.54%), Cross-Site Scripting (0.53%), Cross-Site Request Forgery (0.05%) and http Response Splitting (0.01%).



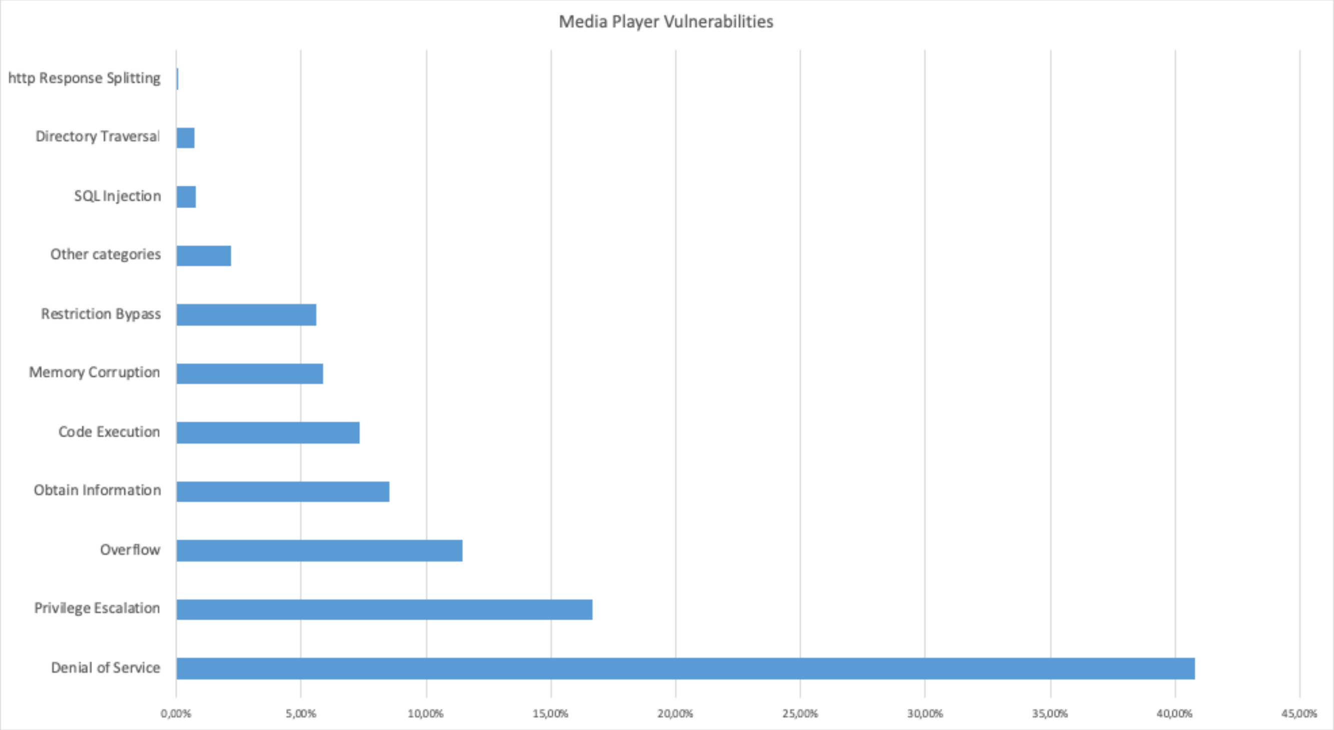
The most common vulnerabilities detected on **computers** are Denial-of-Service (48.44%), Overflow (20.63%), Obtain Information (7.41%), Code Execution (6.69%), Privilege Escalation (4.08%), Memory Corruption (3.55%), Restriction Bypass (2.77%), Directory Traversal (0.57%), Cross-Site Scripting (0.57%), SQL Injection (0.52%), File Inclusion (0.04%) and Cross-Site Request Forgery (0.02%).



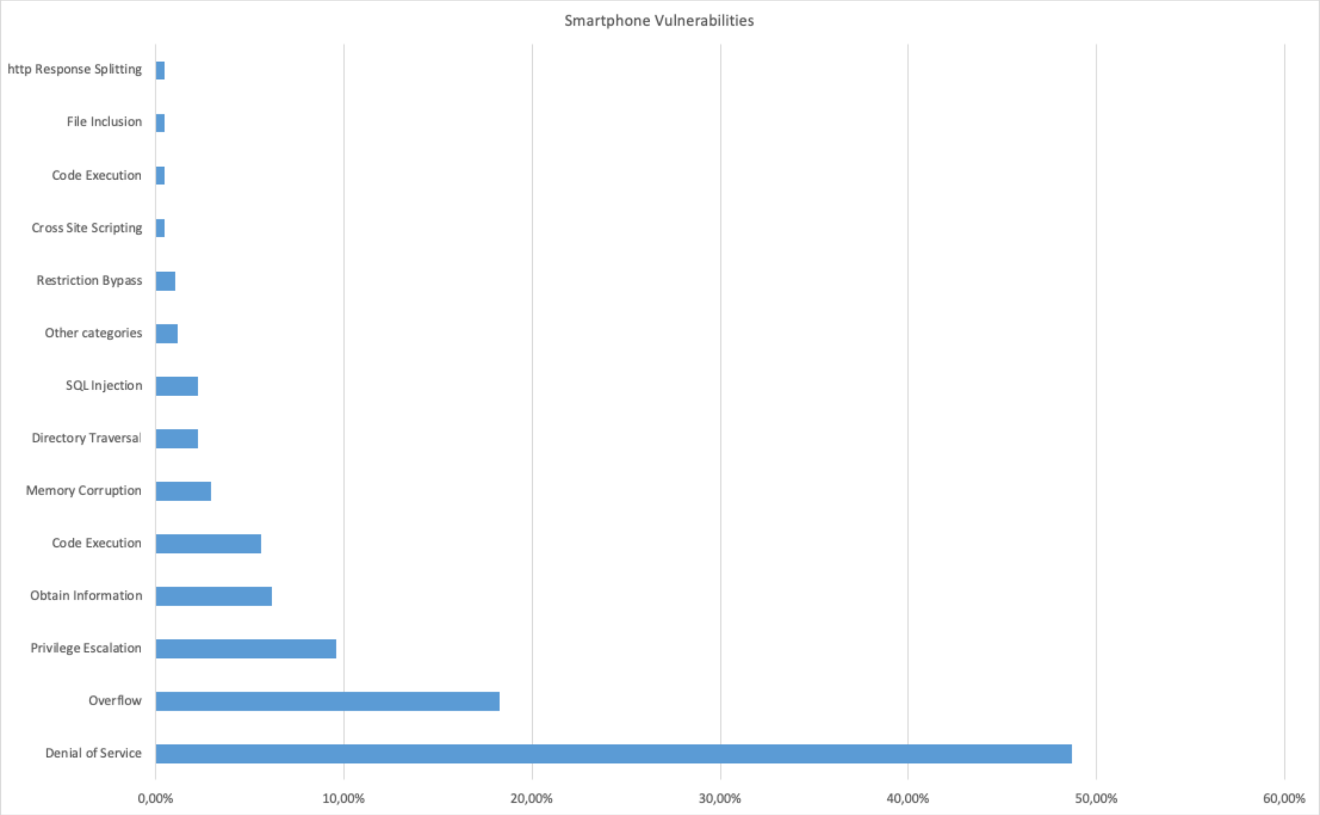
Bitdefender BOX found **IP cameras** to be susceptible to Denial-of-Service (37.33%), Overflow (18.45%), Code Execution (10.37%), Obtain Information (6.83%), Restriction Bypass (5.87%), SQL Injection (4.38%), Privilege Escalation (4.07%), Directory Traversal (3.25%), Memory Corruption (1.78%) and Cross-Site Scripting (1.13%).



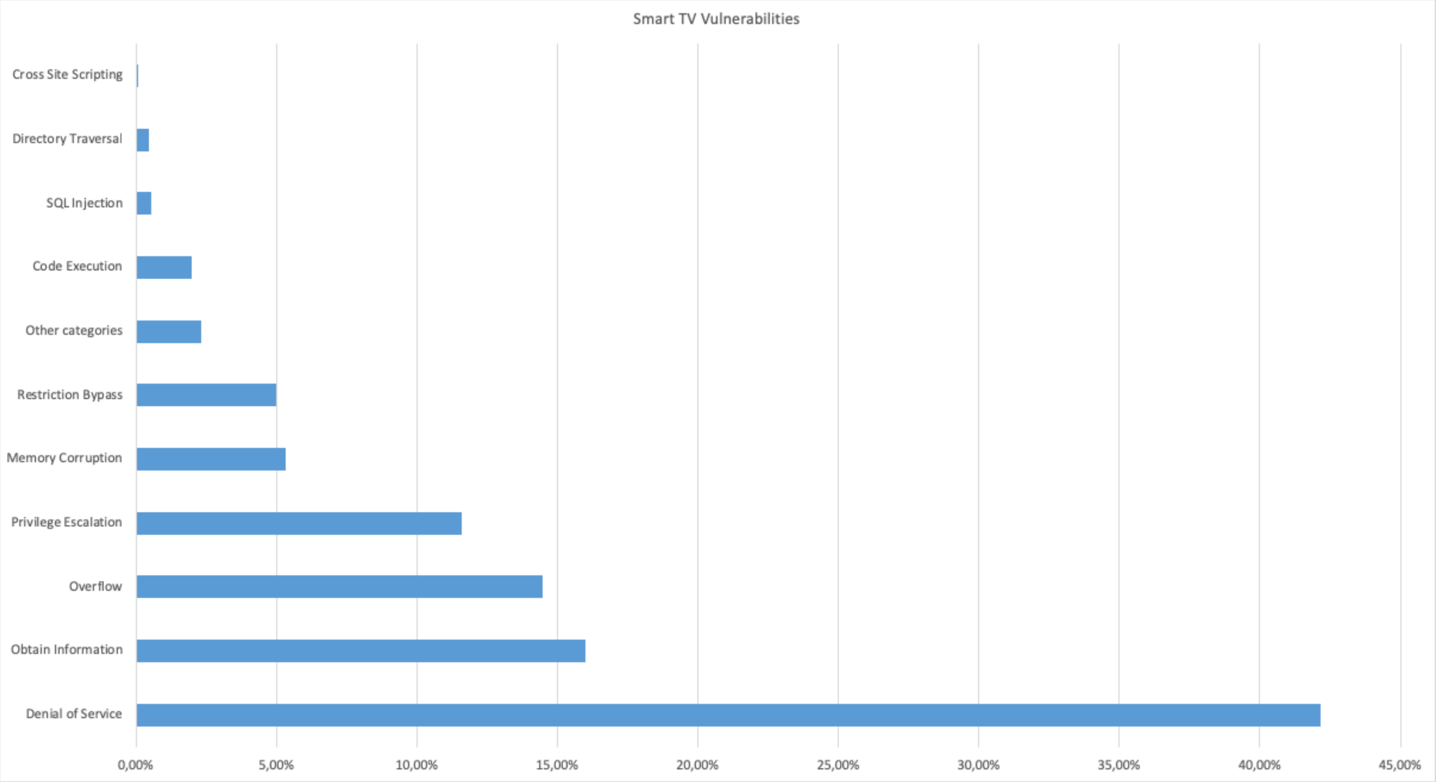
The most common vulnerabilities detected on **media players** are Denial-of-Service (40.79%), Privilege Escalation (16.65%), Overflow (11.46%), Obtain Information (8.51%), Code Execution (7.35%), Memory Corruption (5.89%), Restriction Bypass (5.60%), SQL Injection (0.77%), Directory Traversal (0.72%) and http Response Splitting (0.05%).



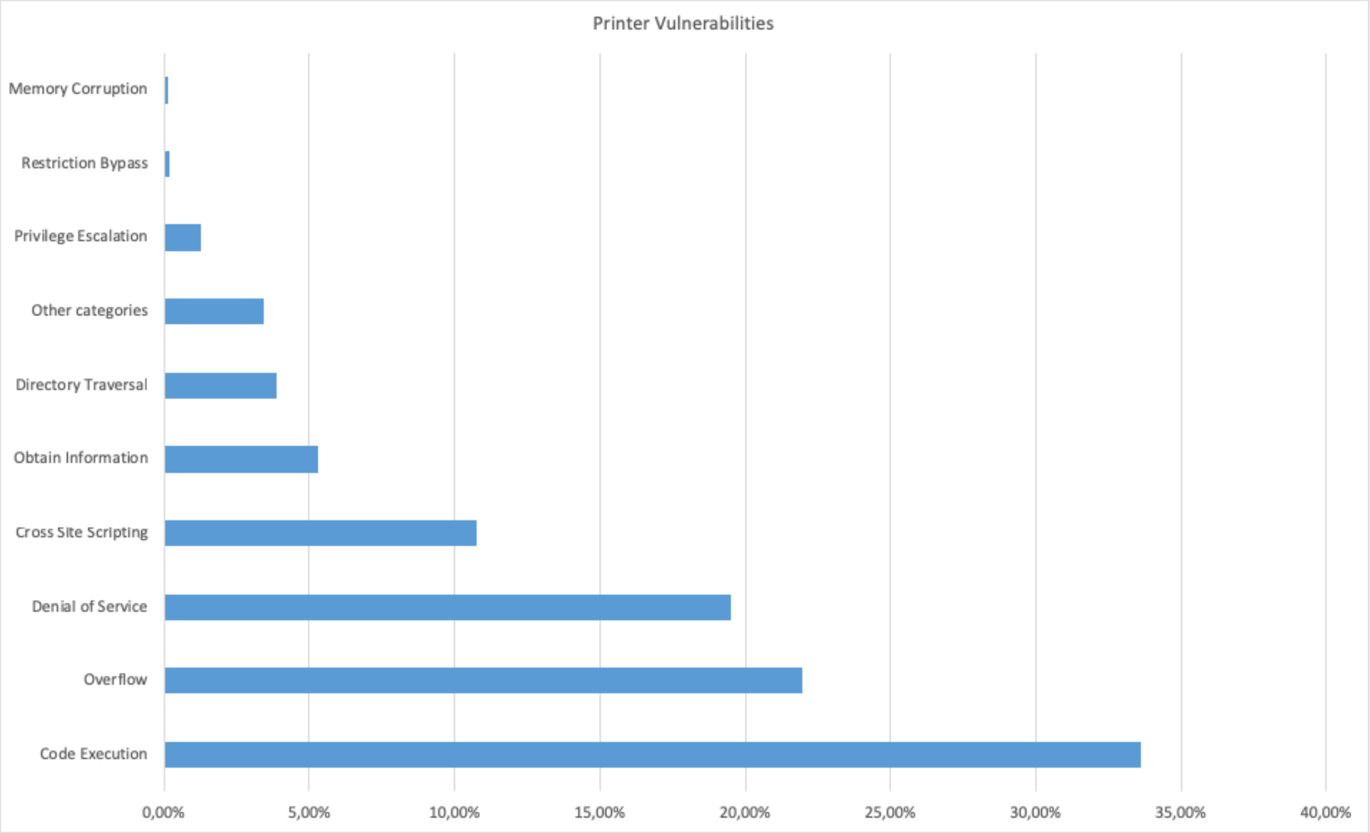
Smartphones were found vulnerable to Denial-of-Service (48.69%), Overflow (18.29%), Privilege Escalation (9.62%), Obtain Information (6.18%), Code Execution (5.58%), Memory Corruption (2.97%), Directory Traversal (2.26%), SQL Injection (2.26%), Restriction Bypass (1.07%), Cross-site Scripting (0.48%), Code Execution (0.48%), File Inclusion (0.48%) and http Response Splitting (0.48%).



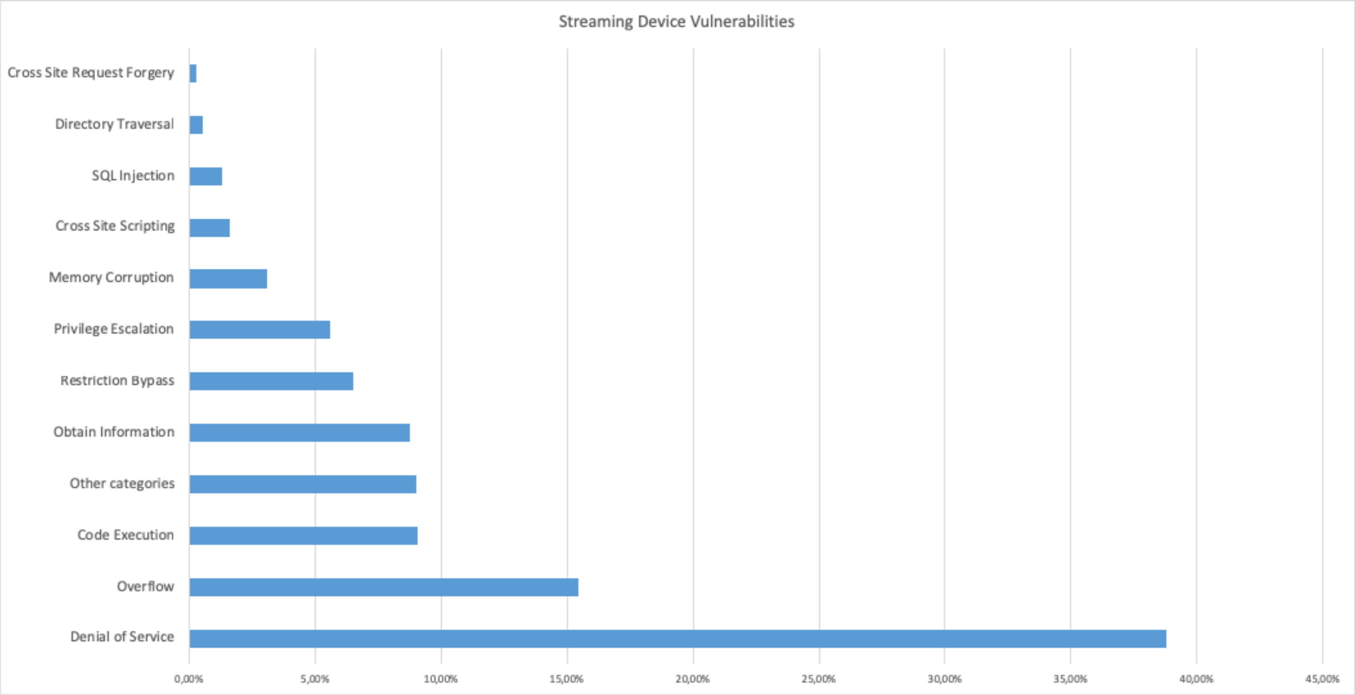
The most common vulnerabilities detected on **smart TVs** are Denial-of-Service (42.17%), Obtain Information (16.00%), Overflow (14.49%), Privilege Escalation (11.60%), Memory Corruption (5.30%), Restriction Bypass (5.00%), Code Execution (1.98%), SQL Injection (0.56%), Directory Traversal (0.47%) and Cross-Site Scripting (0.09%).



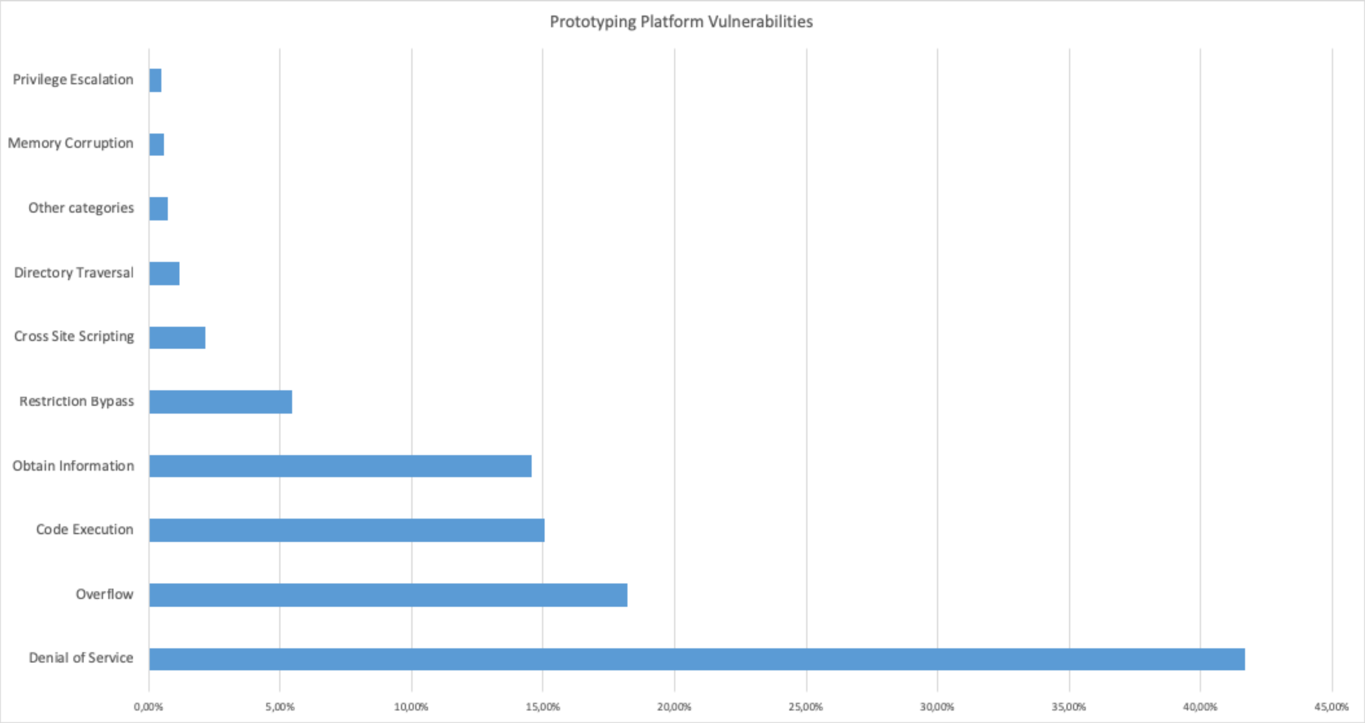
The top vulnerabilities detected on **printers** are Code Execution (33.62%), Overflow (21.95%), Denial-of-Service (19.51%), Cross-Site Scripting (10.74%), Obtain Information (5.28%), Directory Traversal (3.89%), Privilege Escalation (1.28%), Restriction Bypass (0.17%) and Memory Corruption (0.12%).



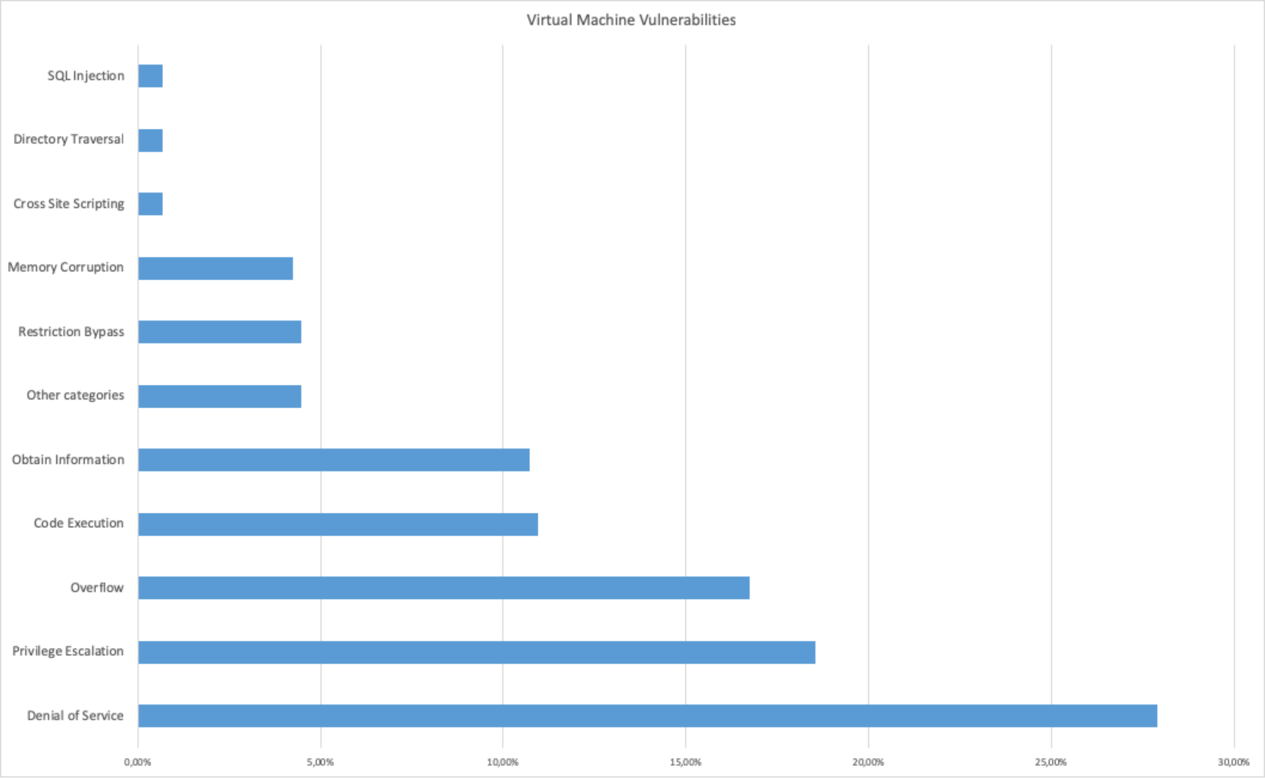
The most common vulnerabilities detected on **streaming devices** (for example, Chromecast, Apple TV, Amazon Fire, Roku Streaming Stick) are Denial-of-Service (38.76%), Overflow (15.43%), Code Execution (9.07%), Obtain Information (8.76%), Restriction Bypass (6.51%), Privilege Escalation (5.58%), Memory Corruption (3.10%), Cross-Site Scripting (1.63%), SQL Injection (1.32%), Directory Traversal (0.54%) and Cross-Site Request Forgery (0.31%).



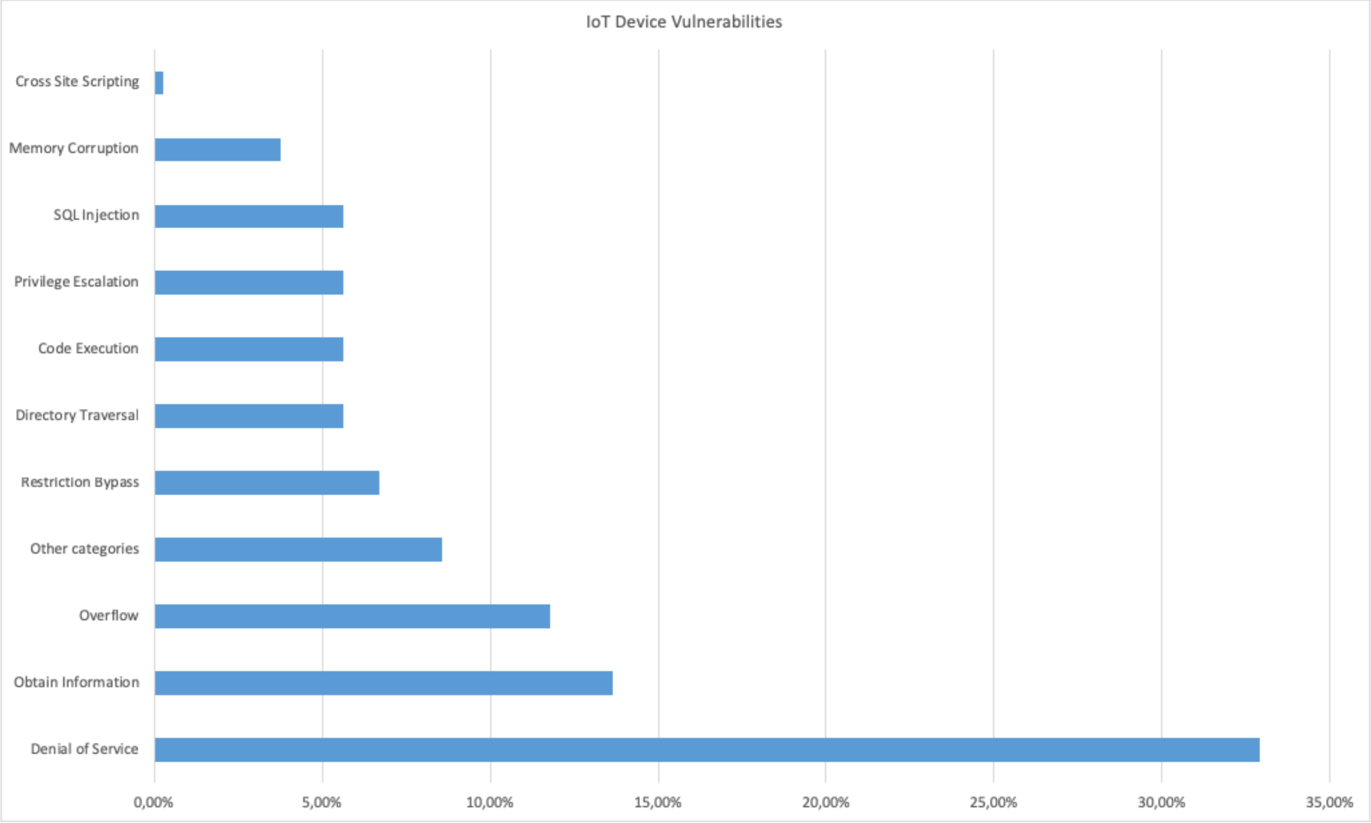
The most common vulnerabilities detected on **prototyping platforms** (Raspberry Pi, Arduino etc) are Denial-of-Service (41.66%), Overflow (18.22%), Code Execution (15.03%), Obtain Information (14.56%), Restriction Bypass (5.44%), Cross-Site Scripting (2.13%), Directory Traversal (1.18%), Memory Corruption (0.59%) and Privilege Escalation (0.47%).



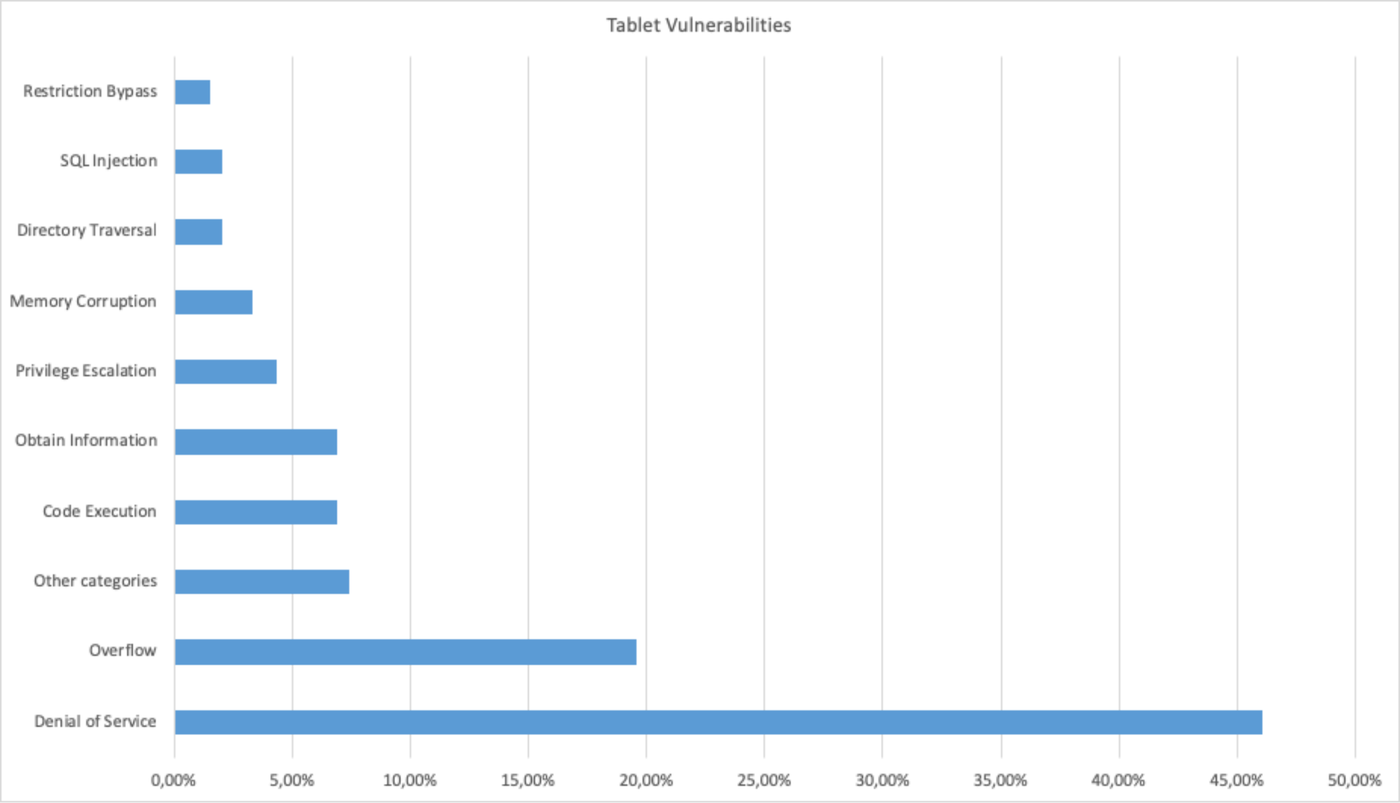
The most common vulnerabilities found on **virtual machines** are Denial-of-Service (27.90%), Privilege Escalation (18.53%), Overflow (16.74%), Code Execution (10.94%), Obtain Information (10.71%), Restriction Bypass (4.46%), Memory Corruption (4.24%), Cross-Site Scripting (0.67%), Directory Traversal (0.67%) and SQL Injection (0.67%).



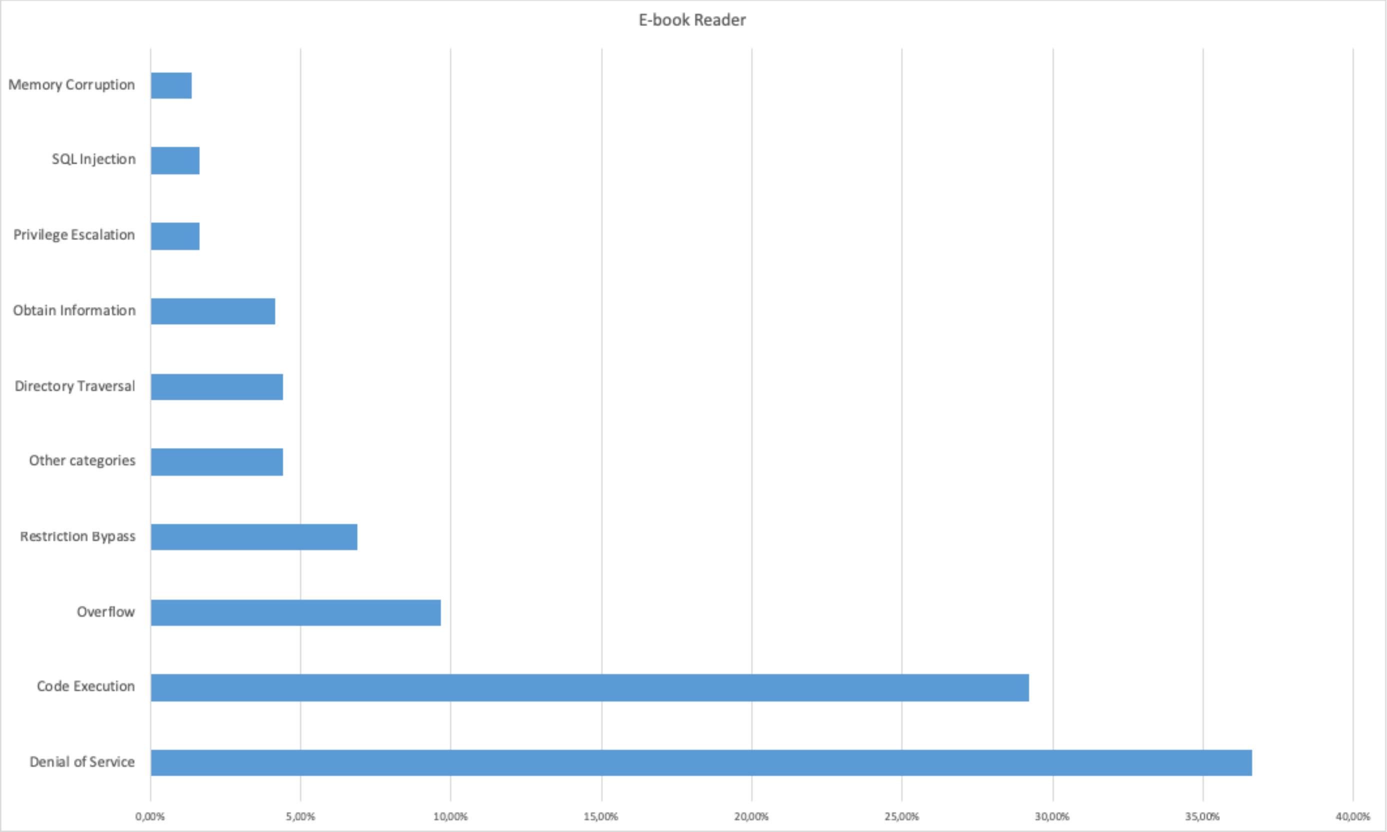
The most common vulnerabilities of **new-generation IoT devices** are Denial-of-Service (32.89%), Obtain Information (13.64%), Overflow (11.76%), Restriction Bypass (6.68%), Directory Traversal (5.61%), Code Execution (5.61%), Privilege Escalation (5.61%), SQL Injection (5.61%), Memory Corruption (3.74%) and Cross-Site Scripting (0.27%).



The most common vulnerabilities detected on **tablets** are Denial-of-Service (46.06%) and Overflow (19.59%), followed by Code Execution (6.87%), Obtain Information (6.87%), Privilege Escalation (4.33%), Memory Corruption (3.31%), Directory Traversal (2.04%), SQL Injection (2.04%) and Restriction Bypass (1.53%).



The most common vulnerabilities detected on **e-book readers** are Denial-of-Service (36.64%) and Code Execution (29.20%), followed by Overflow (9.64%), Restriction Bypass (6.89%), Directory Traversal (4.41%), Obtain Information (4.13%), Privilege Escalation (1.65%), SQL Injection (1.65%) and Memory Corruption (1.38%).



Conclusion

It is no longer only about the theft of private data or video surveillance, but about users unknowingly contributing to the takedown of corporations, government agencies and even the internet, as was seen with Mirai, WannaCry and NotPetya/Goldeneye. Throughout 2017, IoT attacks, cryptomining and ransomware were top threats, and the activity may continue throughout 2018.

Without actively making informed decisions regarding the security status of their home network IoTs, users will be at constant risk of more than just having their private and personal data stolen, leaked, or irreversibly lost. While IoT security awareness should start with manufacturers, it’s also up to individual users to secure their home network and understand the risks associated with poorly secured smart things.

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at
http://www.bitdefender.com/

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com