THE 2024 IOT SECURITY LANDSCAPE REPORT

Bitdefender | NETGEAR

WWW.BITDEFENDER.COM/IOT

ABOUT THIS REPORT

As the creator of the world's first smart home cybersecurity hub, Bitdefender has built extensive experience in detecting, analyzing, and mitigating malware, including threats that are particularly targeting the IoT sector. Our IoT Research team is regularly publishing reports, whitepapers, and blog posts that provide valuable insights into emerging threats, attack techniques, and best practices for securing IoT devices.

At its core, Bitdefender develops advanced malware detection technologies, including machine learning algorithms and behavioral analysis techniques, which are specifically designed to identify and neutralize IoT threats of all kinds. Our expertise in developing and refining these technologies gives us a unique perspective on the evolving IoT security landscape.

This research paper is part of a broader program that aims to offer insight into the modern smart home and the constantly evolving threats that target it.

The information presented here is based on threat intelligence sampled from **3.8 million smart homes** around the world protected by NETGEAR Armor powered by Bitdefender. We investigated about **50 million IoT devices** generating more than **9.1 billion security events** around the world to uncover vulnerabilities and attack scenarios and make the smart home a safer environment for everybody.

THE THREE MILLION TOOTHBRUSHES

In February, a Swiss publication ran a controversial news story regarding three million smart toothbrushes that got hacked into to create a massive DDoS botnet targeting a Swiss organization.

The story gained attention across various media outlets, but it has raised eyebrows among cybersecurity professionals, as lack of technical evidence and missing prerequisites disproved that a large-scale botnet could have been created using toothbrushes.

The idea of three million toothbrushes being hacked to create a massive botnet briefly brought some interesting questions about the Internet of Things security back into the spotlight.

Those three million toothbrushes are a drop in the ocean.

While the toothbrush botnet may seem novel and exciting, it would have been yet another botnet similar to other networks of compromising IoT devices.

The key factors are the vulnerabilities in the devices themselves and the ability of attackers to exploit them, rather than the specific type of device.

And there is no shortage of exploitable devices.

Analyst estimates reveal that more than 15 billion devices are currently connected to the Internet: consumer electronics, industrial equipment, healthcare devices, smart home appliances, and more. Some of these devices have unveiled significant vulnerabilities on the workbenches of our IoT research team, while others have passed the security test with flying colors.

This report looks into the state of the smart home, examining the most frequently seen vulnerabilities and the most popular vulnerable devices. By shedding light on these issues, we aim to equip readers with insights into the evolving landscape of IoT security and empower them to navigate the complexities of securing their connected environments.

KEY FINDINGS & STATS

Every 24 hours, Bitdefender smart home security solutions block an average of 2.5 million threats, or roughly 1736 threats per minute.

3.8 million households

sending 9.1 billion security events and helping paint a clearer picture of what the smart home looks like in 2024

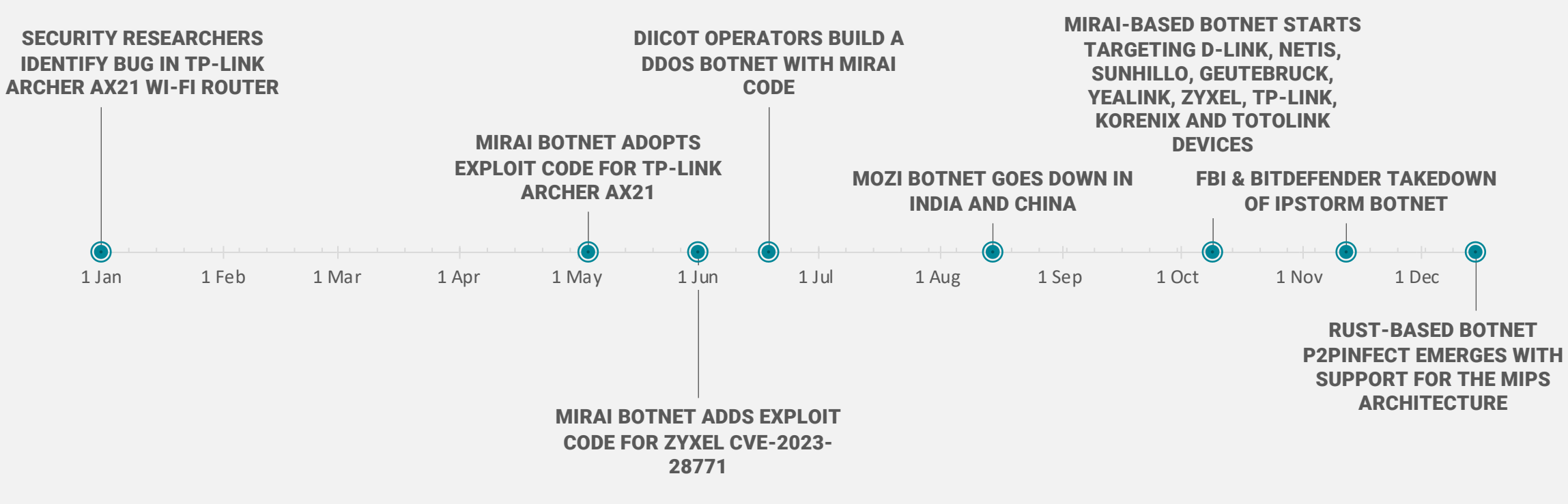
21 devices per household

on average, households own 21 connected devices

10+ attacks every 24h

Home network devices see an average of 10 attacks against connected devices every 24 hours

NOTABLE IOT INCIDENTS IN 2023



THE EYE OF THE INTERPLANETARY STORM

Since 2019, the Bitdefender DRACO team has been monitoring the newly-emerged Interplanetary Storm (IPStorm) Botnet. This anonymization proxy-network-as-a-service infrastructure had been built to be rented out to other cybercrime groups.

Between June 2019 and December 2022, Russian-Moldovan national Sergei Makinin has been hacking thousands of internet-enabled devices to increase the botnet's reliability and dark market value.

The operation to dismantle IPStorm's infrastructure was a collaborative effort involving the Spanish National Police-Cyber Attack Group and law enforcement in the Dominican Republic. Anomali Threat Research and Bitdefender played crucial roles in identifying the malware and providing valuable information leading to Makinin's capture.

"On 15 October 2020, Bitdefender DRACO team was publishing an extensive white paper on the IPStorm Botnet, 'Looking Into the Eye of the Interplanetary Storm'. The last phrase of the document was "More information about this threat actor can be freely provided to law enforcement agencies by reaching out to draco@bitdefender.com". Well, law enforcement did reach out and we provided technical assistance and valuable actionable intelligence on the potential identity of the suspect."

Alexandru Catalin Cosoi, Chief Security Strategist at Bitdefender

UNDERSTANDING THE SMART HOME

A look at the most popular devices, and the top vulnerabilities affecting them

7

Bitdefender | NETGEAR

JUNE 28, 2024

A TYPICAL SMART HOME

In 2023, a typical smart home mostly consists of interconnected devices and systems designed to enhance convenience, security, energy efficiency, and comfort.

On top of this foundation (the visible "surface" of devices purchased and installed by owners and tenants), modern buildings come pre-fitted with a vast range of automations, meters and sensors that are out of sight: smart meters, smart circuit breakers, smoke and humidity sensors.

27%

STREAMING DEVICE / TV

Be it dedicated sticks or Android-based boxes, streaming devices are wildly popular.

28%

MOBILE PHONE /TABLET

One in four devices is a mobile phone.

12%

COMPUTER OR LAPTOP

Once the apex of the connected world, laptops and PCs are now outnumbered by "things."

2%

CONSOLE

Most of the monitored smart homes have a game console connected to the Internet.

31%

OTHERS

The vast majority of connected devices range from smart switches and lightbulbs, to treadmills and aquariums.

COUNTING VULNERABILITIES

Today's modern devices operate using intricate technology stacks and heavily depend on cloud connectivity to carry out their smart functions. This combination of firmware and hardware creates a significant footprint susceptible to attacks.

When considering vulnerabilities, it's crucial to understand that defining the 'most vulnerable' device involves various metrics. For instance, a widely used gadget may only have one vulnerability, while a less mainstream device could be impacted by numerous issues.

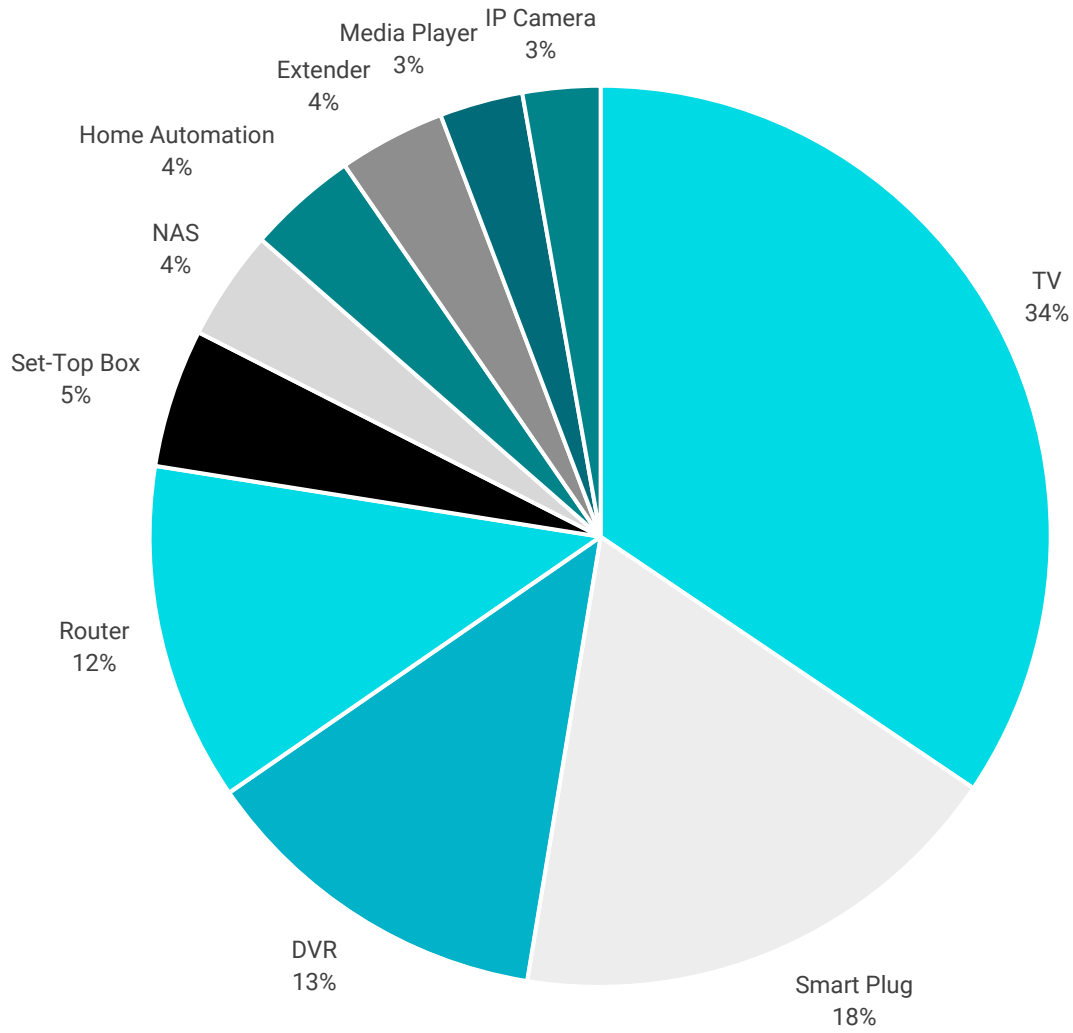
Whether the weakness lies in the sheer number of vulnerable devices or in multiple implementation errors on a less prevalent make and model, our technologies can help protect the user.

DEVICES BY VULNERABILITY COUNT

In 2023, the highest number of vulnerabilities were discovered in TV sets, smart plugs, and digital video recorders.

Vulnerabilities in TVs are quite common, largely due to their extended lifespan and the tendency for manufacturers to discontinue support while the devices are still in use.

Consequently, newly identified vulnerabilities often remain unaddressed (known as 'n-days') until the device is no longer in service.



VULNERABILITIES AND DEVICES (I)

Upon analysing the data, several intriguing patterns emerge regarding the total number of vulnerabilities across various device types.

TV sets stand out with a staggering total of vulnerabilities, despite being fewer in number compared to other devices like routers and IP cameras. This discrepancy suggests that TVs might possess inherently complex systems or face unique security challenges that lead to a higher vulnerability count per device.

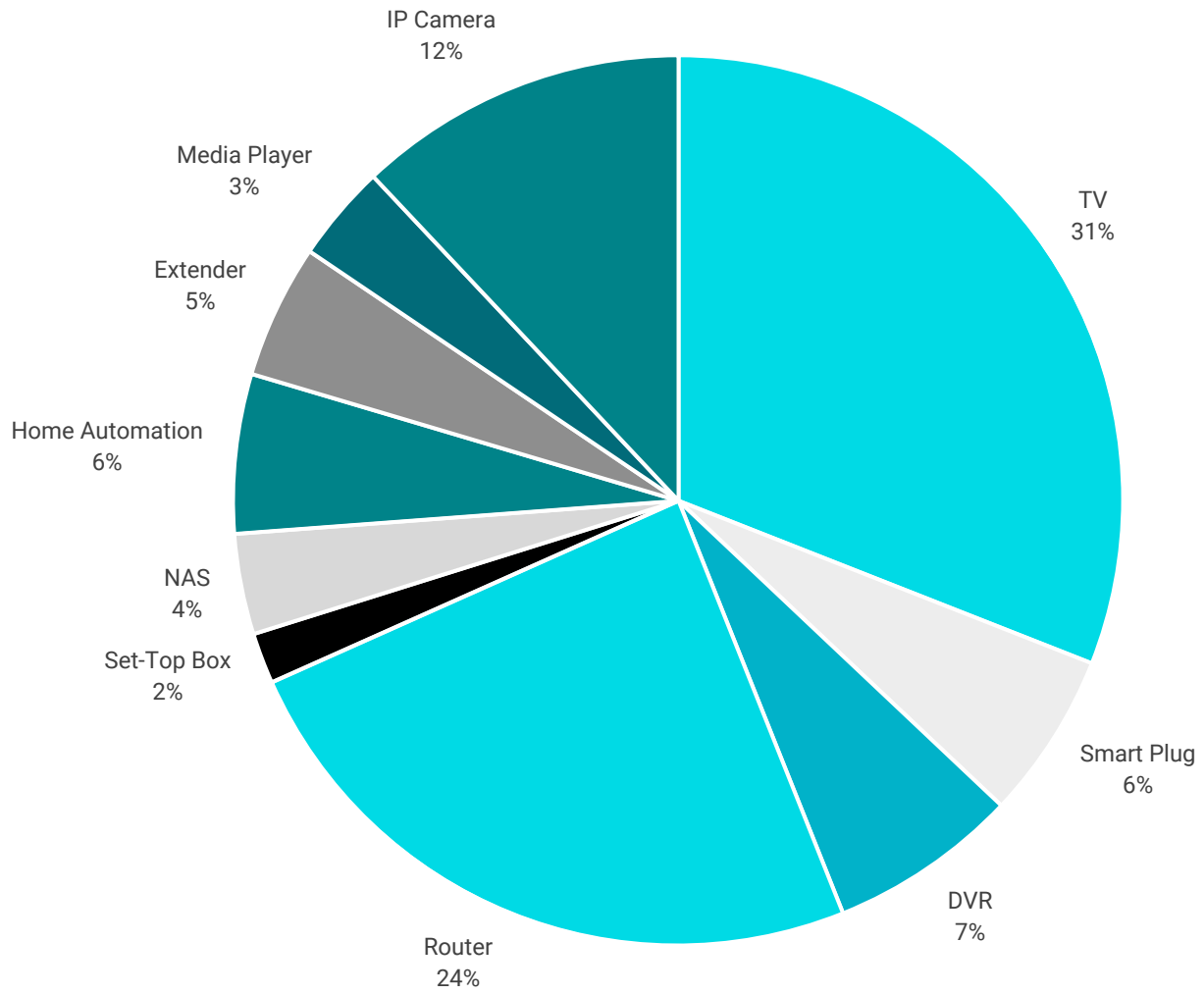
Moreover, the high number of vulnerabilities in TV sets underscores the importance of robust security measures in consumer electronics, particularly considering the potential risks associated with devices that often have access to sensitive information, have a long life span and are tightly integrated with sensitive components of the home network (such as NAS devices or other mass storage media).

VULNERABLE DEVICES BY DEVICE COUNT

In terms of vulnerabilities per device, Smart TVs still hold the number one position, likely due to the fact that they are widely present in each home in greater numbers.

Vulnerabilities in TVs are quite common, largely because of their extended lifespan and the tendency for manufacturers to discontinue support while the devices are still in use.

Consequently, newly identified vulnerabilities often remain unaddressed (known as 'n-days') until the device is no longer in service.



VULNERABILITIES AND DEVICES (II)

Smart Plugs and digital video recorders (DVRs) exhibit substantial vulnerability counts relative to their respective device populations. While Smart Plugs serve as convenient additions to smart home setups, their vulnerability count highlights potential security weaknesses in these seemingly innocuous devices.

Likewise, vulnerabilities in DVRs raise concerns about the security of video surveillance systems commonly employed in both residential and commercial settings. These findings emphasize the need for manufacturers to prioritize security in the design and production of such devices, as they play integral roles in modern connected environments.

Furthermore, the relatively low vulnerability counts in devices like set-top boxes and network-attached storage (NAS) units indicate varying levels of security posture across different categories of consumer electronics, warranting tailored approaches to mitigate potential risks and safeguard user data and privacy.

OBSERVATIONS AND TRENDS

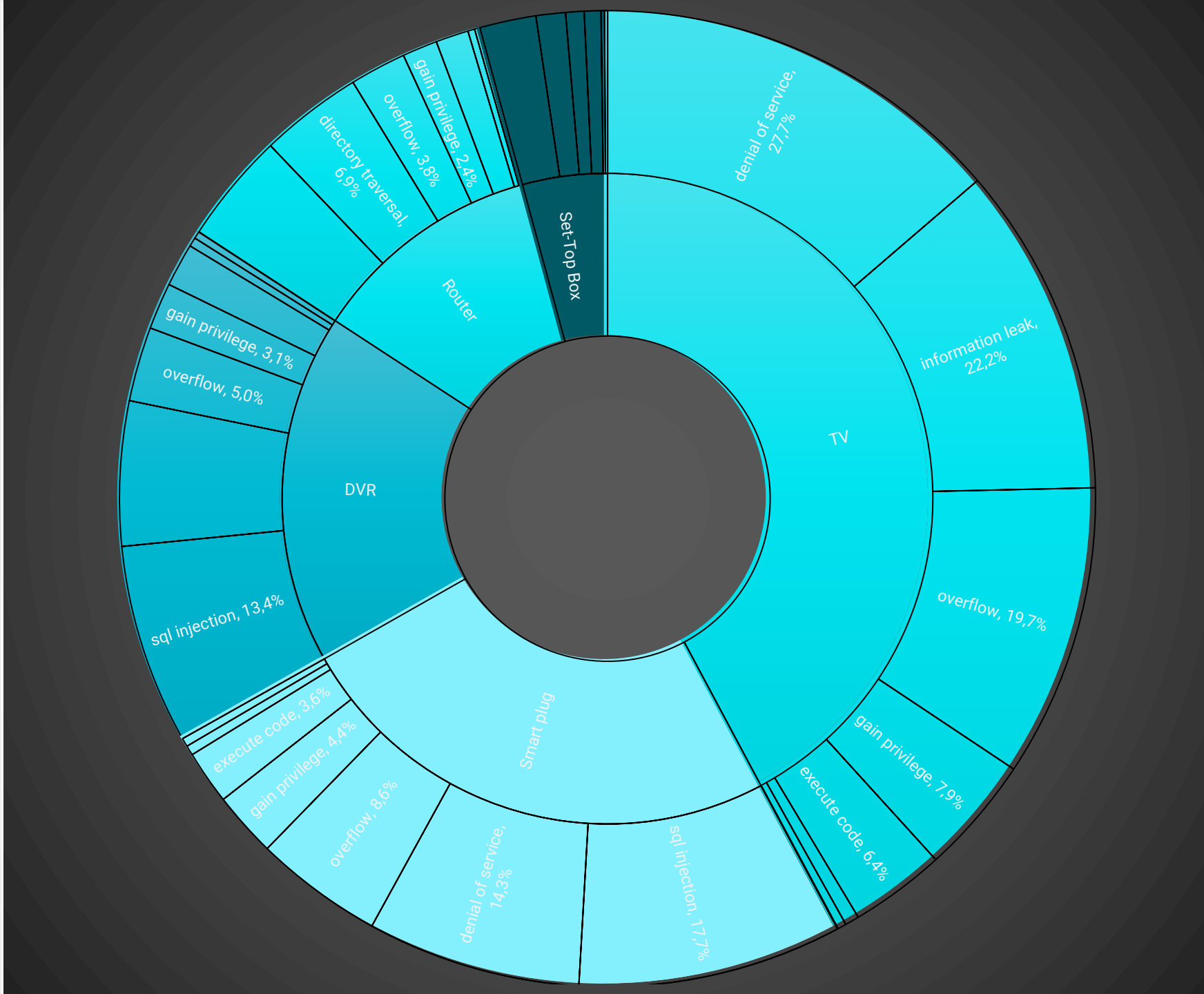
Complexity and Functionality: Devices like TV sets and DVRs, which often have sophisticated features such as internet connectivity and multimedia capabilities, tend to have higher vulnerability counts compared to simpler devices like set-top boxes. This suggests that the more features and functionalities a device has, the greater the potential attack surface and hence vulnerability count.

Industry Standards and Security Practices: Certain industries or product categories adhere to better security standards and practices, resulting in lower vulnerability counts. For instance, devices categorized under "Home Automation" might have relatively fewer vulnerabilities compared to other categories due to standardized security protocols and certifications in the home automation industry.

Manufacturer Practices: The number of vulnerabilities also varies based on the practices of device manufacturers. Devices from manufacturers that prioritize security in their design, development, and patching processes may exhibit lower vulnerability counts compared to those from manufacturers that are less focused on security.

DEVICES BY VULNERABILITY TYPE

Overall, the data highlights the complexity of cybersecurity threats facing various device types and underscores the importance of proactive measures to address vulnerabilities and safeguard user data and privacy in the increasingly interconnected digital landscape.



INSIGHTS

Several insights can be extrapolated regarding the types of vulnerabilities present in different device types:

Prevalent Vulnerability Types: Across all device types, denial of service (DoS) attacks appear to be the most common type of vulnerability, with significant percentages observed for TV sets (36.7%), Smart Plugs (22.2%), DVRs (17.7%), routers (13.4%), and Set-Top Boxes (6.9%). This shows that DoS vulnerabilities are widespread across various device categories and pose significant risks to their availability and functionality.

Severity of Exploitable Vulnerabilities: Vulnerabilities categorized as overflow and gaining privilege follow denial of service as the next most prevalent types across most device categories. These vulnerabilities can potentially enable attackers to execute arbitrary code or gain unauthorized access to device resources, highlighting their severity and the importance of addressing them promptly.

Variation in Vulnerability Distribution: While denial of service vulnerabilities are consistently prevalent across different device types, the distribution of other vulnerability types varies. For example, TV sets exhibit a higher percentage of overflow vulnerabilities compared to other device types, suggesting potential weaknesses in memory management or input validation mechanisms specific to TVs.

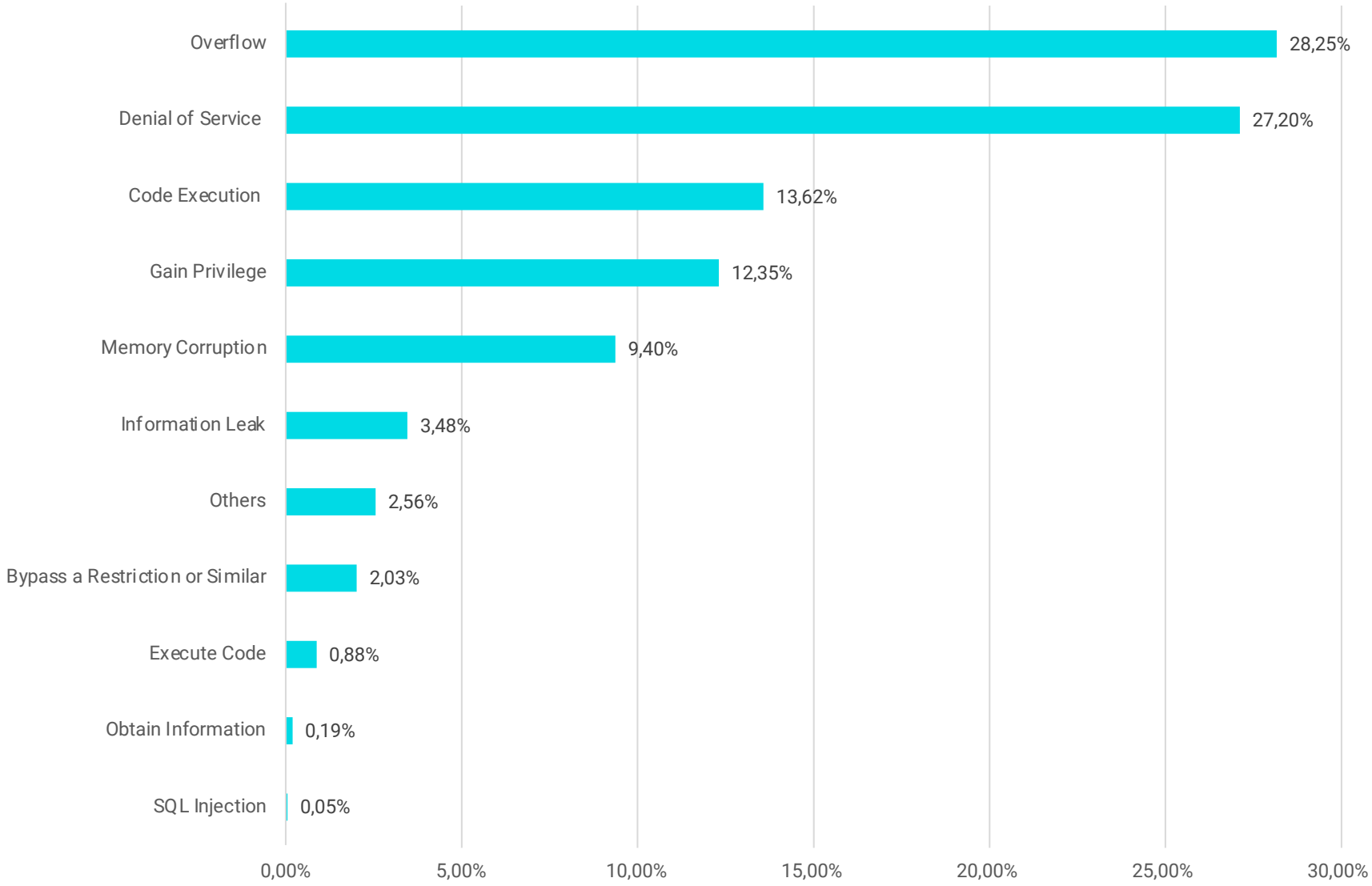
Need for Mitigation Strategies: The presence of diverse vulnerability types underscores the importance of implementing comprehensive security measures, including regular software updates, vulnerability assessments, and penetration testing at the vendor level to mitigate potential risks and enhance the overall security posture of connected devices.

VULNERABILITIES BY TARGETED OUTCOME

Smart devices have different functions or hardware capabilities and therefore, different threat models.

While some devices are connected to the network and wait for instructions, others are actively sending out data.

Consequently, the attacks against these devices and their intended outcome vary.



IMPACT

Looking at the vulnerability distribution by targeted outcome reveals that **buffer overflow** and **denial of service** vulnerabilities are the most prevalent, collectively accounting for over half of all vulnerabilities identified. This shows that buffer overflow and service disruption are widespread security concerns across various device types.

Code execution and gaining privilege vulnerabilities, while less common than overflow and denial of service, pose significant risks due to their potential to allow attackers to execute arbitrary code or gain elevated privileges on compromised devices. These vulnerabilities can lead to unauthorized access, data breaches, and system compromise.

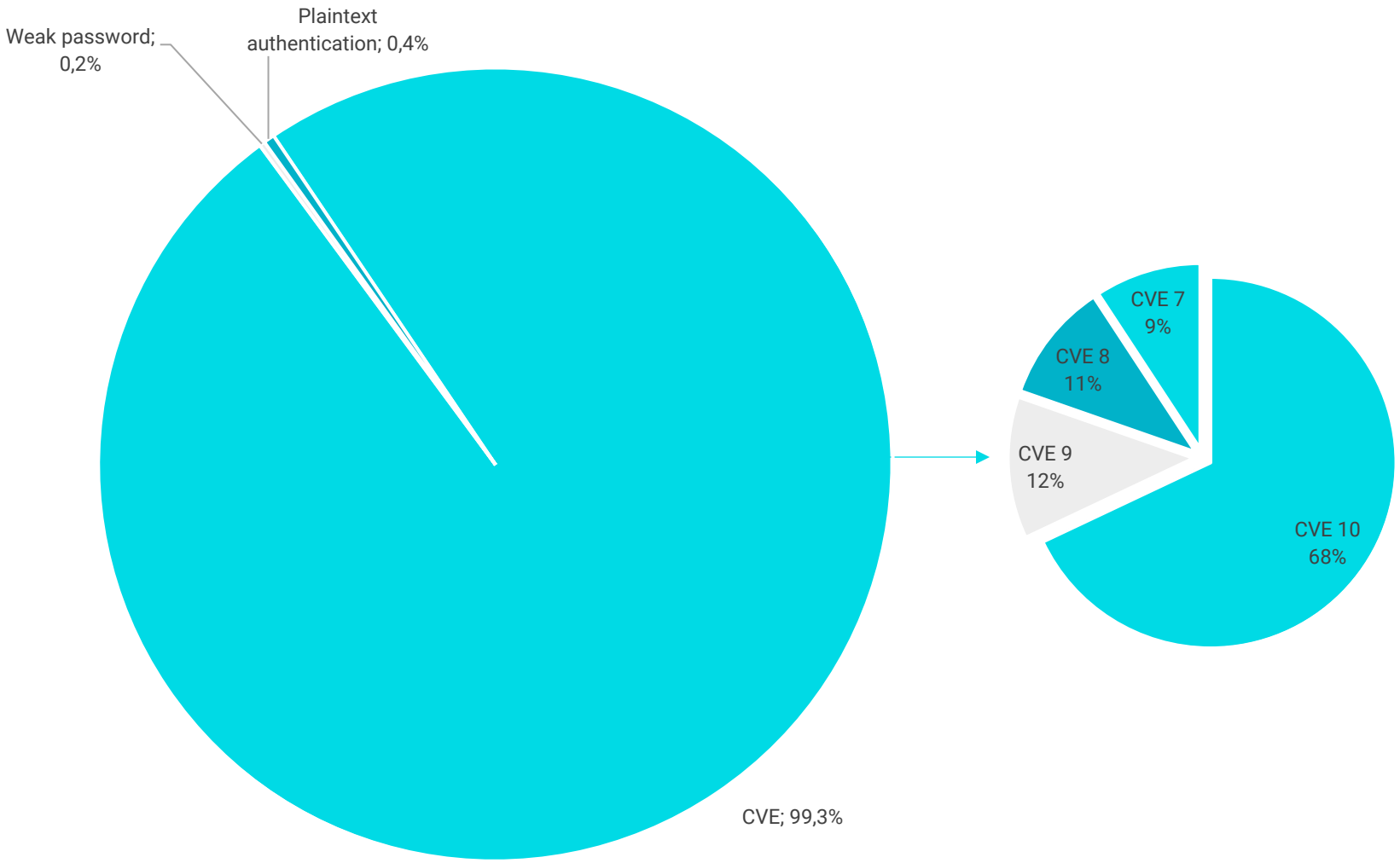
Memory corruption vulnerabilities, though less prevalent than **overflow** and **denial of service**, remain a notable concern, given their potential to exploit weaknesses in memory management systems and their contribution towards arbitrary code execution attacks. Mitigating memory corruption vulnerabilities requires thorough code review, input validation, and memory protection mechanisms to prevent exploitation.

VULNERABILITY TYPES AND RISK VALUES

The overwhelming majority of exploitation attempts against IoT devices rely on previously known (and fixed) CVEs. Only a fraction of attacks leverage weak passwords or plaintext authentication.

Looking closer at the CVE distribution, we see that the vast majority of vulnerabilities have a perfect 10 score which often means total compromise of the device and a CRITICAL security rating.

An interesting aspect is the fact that attackers seem to avoid using exploit code for vulnerabilities rated 6 or lower.



IOT PRIVACY AND SECURITY

The explosion of Internet of Things (IoT) devices has brought about a plethora of security and privacy challenges. Vulnerabilities in popular IoT frameworks that connect devices to their clouds can expose tens of millions of users to privacy risks.

Prime examples are vulnerabilities discovered in the ThroughTek Kalay platform, a widely used IoT solution for device connectivity. This Bitdefender research uncovered critical flaws that could allow attackers to intercept audio and video data, manipulate device functions, and compromise user privacy. Such vulnerabilities highlight the pervasive risks associated with IoT devices, which often suffer from inadequate security measures and slow patching cycles.

To address these concerns, the U.S. government has introduced the Cyber Trust Mark, a certification designed to enhance cybersecurity standards for IoT devices. The Cyber Trust Mark helps consumers identify devices that meet specific security criteria, reducing the risk of purchasing devices that are likely to get hacked.

BEYOND IOT

Legacy devices like smartphones, laptops, and desktops are also at risk. The 2024 Consumer Cybersecurity Assessment Report by Bitdefender surveyed 7,335 consumers across the UK, US, Germany, Spain, France, Italy, and Australia. The report found that 78.3% of respondents use mobile devices for sensitive transactions such as banking and healthcare. However, 44.5% do not use any mobile security solutions, leaving them vulnerable to malware, phishing, and data breaches.

Netgear Armor provides advanced cybersecurity for your home network, securing an unlimited number of IoT devices and offering complete protection for Windows PCs, macOS, Android, and iOS devices. Integrating Netgear Armor can safeguard your sensitive data and protect against various cyber threats.

PREDICTIONS FOR 2024

22 Bitdefender | NETGEAR

JUNE 28, 2024

1

Increased regulatory focus on IoT security standards

In 2024, we can expect to see a significant uptick in regulatory efforts aimed at establishing comprehensive IoT security standards and guidelines. As the number of connected devices continues to proliferate across various industries and sectors, as well as at home, policymakers will prioritize initiatives to mitigate the associated cybersecurity risks and protect consumer privacy.

This will likely involve the introduction of new legislation, mandates, or industry regulations that enforce minimum security requirements for IoT devices, such as encryption protocols, regular security updates, and robust authentication mechanisms. Additionally, regulatory bodies may impose stricter penalties or fines for non-compliance with these standards, incentivizing manufacturers and service providers to prioritize security in their IoT offerings. This regulatory landscape will shape the development and deployment of IoT technologies, driving industry-wide efforts to enhance security and resilience in interconnected ecosystems.

2

Growing emphasis on supply chain security for IoT devices

Supply chain security will emerge as a critical focus area for ensuring the integrity and resilience of IoT devices in 2024. As the IoT ecosystem becomes increasingly interconnected and reliant on third-party components and services, vulnerabilities within the supply chain pose significant risks to device security and functionality.

Organizations will prioritize supply chain risk management practices, including thorough vendor assessments, security audits, and supply chain transparency initiatives to identify and mitigate potential threats throughout the procurement lifecycle. Additionally, there will be greater demand for secure boot processes, code signing, and firmware integrity verification mechanisms to ensure the authenticity and integrity of IoT device firmware and software updates.

Strengthening supply chain security will be essential for safeguarding IoT devices against malicious tampering, counterfeit components, and supply chain compromises that could undermine their security and trustworthiness.

3

Customer security will become the number one priority for ISPs and equipment vendors

Router manufacturers and ISPs benefit from prioritizing IoT security to maintain network integrity, enhance customer trust, ensure regulatory compliance, reduce support costs, and drive market differentiation. Vulnerable IoT devices can compromise network security, eroding customer trust and risking regulatory penalties.

Proactive security measures mitigate these risks, reducing support inquiries and attracting security-conscious customers. By emphasizing IoT security, providers establish themselves as trusted guardians of the digital ecosystem, gaining a competitive edge in the market while preserving network integrity and customer satisfaction.

HOW CAN USERS STAY SAFE

- Both home users and employees should be aware of active IoT devices in their networks and keep them up to date. If some devices are past their end of life, replace them with newer models.
- Move all smart devices to a dedicated guest network to isolate them from the main network.
- Patch devices as soon as a new firmware version becomes available.
- Use routers or gateways with built-in security.
- Probe the home network for vulnerable devices with a smart home scanner.
- Avoid exposing LAN devices to the Internet unless necessary.

This report is based on cyber-security insights received between January 1 and Dec 31, 2022.

ROUTER SECURITY

As crucial Internet infrastructure, routers are exposed to a wide range of security threats. A combination of outdated software, lack of encryption, weak passwords, misconfigured remote management, as well as an overall lack of on-device security mechanisms allows attackers to hijack routers and enroll them into botnets, get into the network and gain control of the connected devices.

With NETGEAR Armor powered by Bitdefender, home users have access to advanced cybersecurity on Orbi mesh WiFi systems and Nighthawk routers.

NETGEAR Armor combines NETGEAR's long-standing pursuit to deliver the fastest & latest connectivity with Bitdefender's award-winning technology to secure all connected devices in every home.


Bitdefender®
WWW.BITDEFENDER.COM/IOT