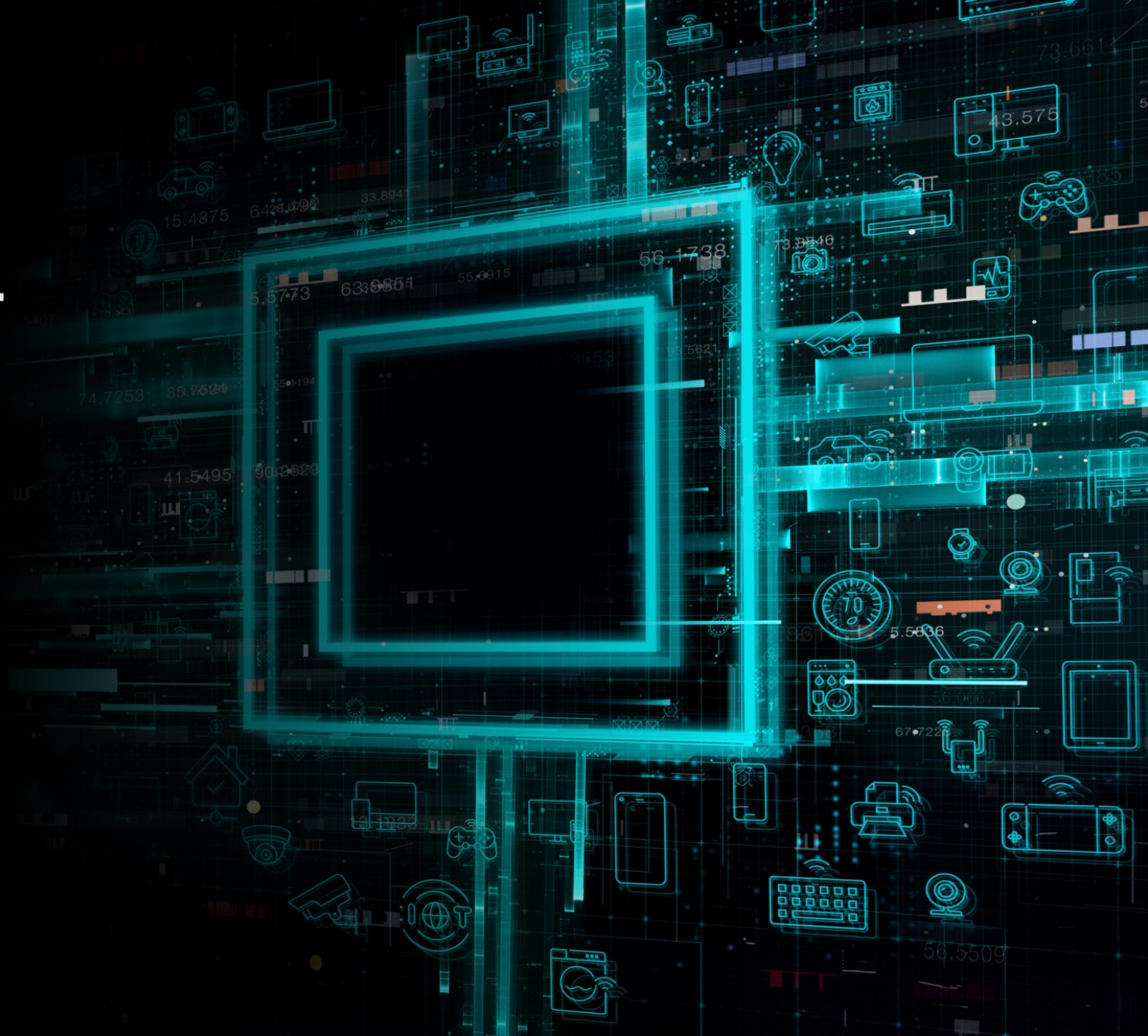
THE 2025 IOT SECURITY LANDSCAPE REPORT



Bitdefender | NETGEAR

WWW.BITDEFENDER.COM/IOT

ABOUT THIS REPORT

Bitdefender has built deep expertise in detecting, analyzing, and mitigating threats across the Internet of Things (IoT) ecosystem. Our IoT Lab monitors global trends and publishes insights into new attack vectors, vulnerability types and best practices for securing connected devices - from smart TVs and routers to wearables and phones.

This report draws on threat intelligence from 6.1 million smart homes across the US, Australia and Europe, protected by Bitdefender IoT Security technologies such as NETGEAR Armor. Our research team examined data from over 58 million IoT devices, analyzing 4.6 billion vulnerabilities* and 13.6 billion IoT attacks to build a precise snapshot of the smart home security landscape. By combining large-scale insights with behavioral analysis, we aim to reveal how modern threats evolve, propagate and exploit the devices we rely on most - and how users can stay ahead of them.

**Bitdefender has blocked 4.6 billion attempts at exploiting non-unique device vulnerabilities. These attempts can leverage one or more known attack vectors multiple times.*

The data used in this report was collected and analyzed between January 1 and October 1, 2025, capturing the most recent developments in IoT threat activity and vulnerability trends. The findings reflect the threat dynamics shaping the smart home ecosystem today.

KEY STATS AT A GLANCE

Bitdefender smart home technologies block 12 million threats a day around the world

6 million households

Sharing information about 13 billion attack attempts on routers and connected devices

22 devices per household

The average household has 22 connected devices

29+ attacks every 24h

Home network devices face an average of 29 attacks on connected devices per day

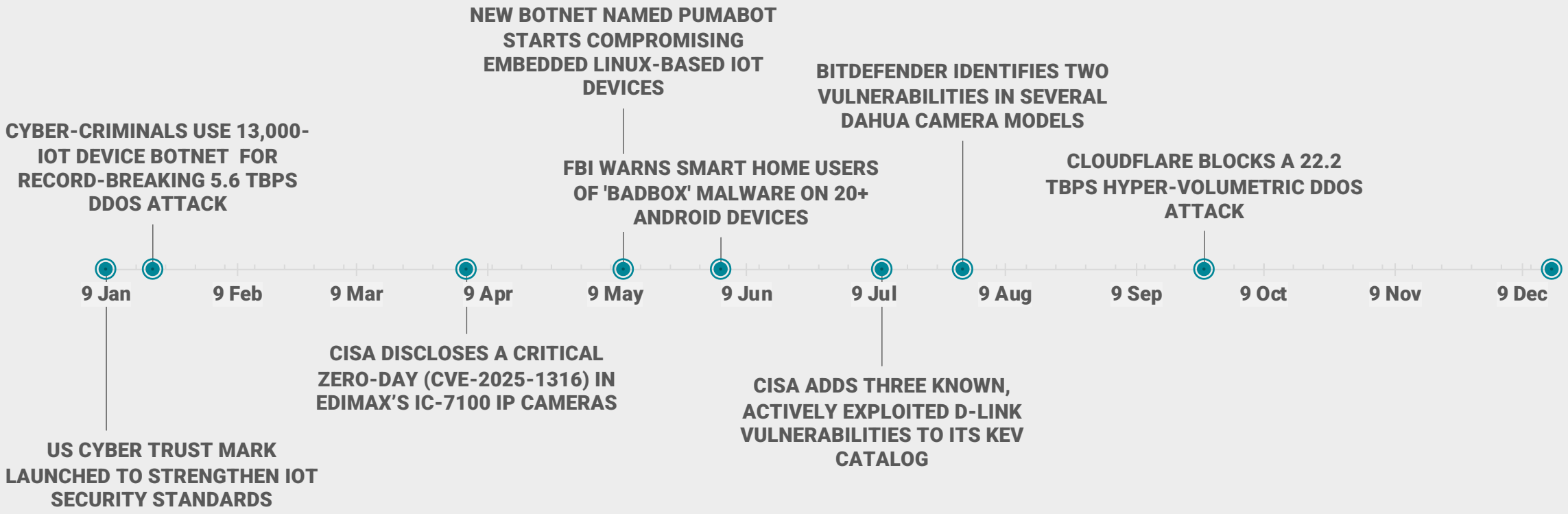
4.6 billion vulnerabilities

This report is based on analysis of 4.6 billion vulnerabilities exploitation attempts against live IoT targets

Bitdefender | NETGEAR

OCTOBER 21, 2025

NOTABLE IOT INCIDENTS IN 2025



SUNLIGHT, PANELS AND A DARK SIDE

In late 2024, our research team uncovered a startling reality: solar inverters – small devices sitting quietly in homes and businesses – could be chained together into an attack force powerful enough to destabilize national power grids.

This is no theoretical risk – it's a real threat. Tens of thousands of inverters were accessible online because of vulnerabilities in device firmware. If compromised, these devices could be commanded to push or pull electricity into the grid in synchronized bursts. That could take down portions of a country's critical infrastructure.

These inverters are technically consumer electronics. They sit in garages, on rooftops and in backyards. They are marketed for their efficiency and eco-friendliness, not resilience against cyberattacks. But when millions of households become miniature power plants, the line between consumer gadget and national infrastructure blurs.

IoT is no longer just about smart homes, baby monitors or lightbulbs. When connected devices control the flow of energy, water or healthcare equipment, they stop being personal conveniences and start being public risks.

Germany has already raised the alarm. With one of the highest rates of solar adoption in Europe, the country is acutely aware that millions of small-scale inverters, each connected to the internet, represent a critical vulnerability. Policymakers and grid operators worry that if attackers synchronized control over these devices, it could ripple across the national grid and disrupt energy stability at scale.

The future grid will be decentralized, green and digital - but it will also be dangerously fragile unless security keeps pace.

IOT FLAWS TURN PRIVATE LIVES INTO PUBLIC SHOW

In one recent case, unsecured smart cameras turned ordinary people into unwitting stars of an underground reality stream broadcast from retail fitting rooms, swimming pools and private homes in Italy. *Read the reporting by Corriere della Sera (in Italian)*

In June 2025, five men were convicted of distributing thousands of hours of footage taken from compromised surveillance cameras. Private moments were streamed and shared across Telegram and other platforms, often with degrading comments and location tags. Most victims still don't know they were filmed.

These weren't state-sponsored hackers or corporate-grade intrusions. This was voyeurism at scale, enabled by a common flaw in the form of unsecured IoT surveillance camera devices.

Cheap, poorly configured cameras promise security but deliver the opposite. Devices exposed to the internet, left with factory-default credentials, or manufactured with poor security practices become open doors. In the Milan case, the attackers weren't hacking wizards. They were simply patient enough to scan the internet for publicly accessible cameras.

22.2 TBPS – THE RISE OF ROUTER BOTNETS

In September 2025, Cloudflare reported a 22.2 terabit-per-second distributed denial-of-service (DDoS) attack - the largest in history. The event, which lasted only 40 seconds, generated over 10.6 billion packets per second, a torrent of malicious traffic equivalent to streaming a million 4K videos at once.

The assault was autonomously detected and mitigated, setting a new benchmark for both attack scale and defense automation. While the culprits are not yet known, the scale and coordination suggest a link to hyper-volumetric botnets built from compromised routers and IoT devices.

The AISURU botnet, uncovered by QiAnXin's XLab, shows how large-scale exploitation of consumer-grade networking gear can generate unprecedented attack volumes. AISURU enslaved hundreds of thousands of routers worldwide, combining them into a weaponized mesh that saturates backbone links and overwhelms infrastructures.

The 22.2 Tbps incident highlights the shifting power balance between consumer IoT exploitation and core Internet stability. It's yet another reminder that IoT devices - not data centers - are now the backbone of global cyber offense, and that the line between residential compromise and disruption of critical infrastructure grows thinner every year.

SMART HOME TRENDS IN 2025

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

Bitdefender | NETGEAR

OCTOBER 21, 2025

THE SMART HOME

The smart home ecosystem is dominated by mobile devices and screens, with phones representing nearly 20% of all connected endpoints – more than double the share of smart TVs. This reflects a shift: the smartphone has become the universal remote for the digital household.

Together with TVs, streaming devices, and tablets, entertainment and content consumption hardware make up more than a third of all connected nodes – convenience and leisure still drive most IoT adoption.

20%

MOBILE PHONES

More than just a tool for voice communication, this device integrates all aspects of modern life

10%

TV SETS

From screens to media servers: smart TVs now do far more than just play movies.

10%

COMPUTERS & LAPTOPS

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

7%

STREAMING DEVICES

Tiny sticks, massive reach: entertainment in every port and socket.

53%

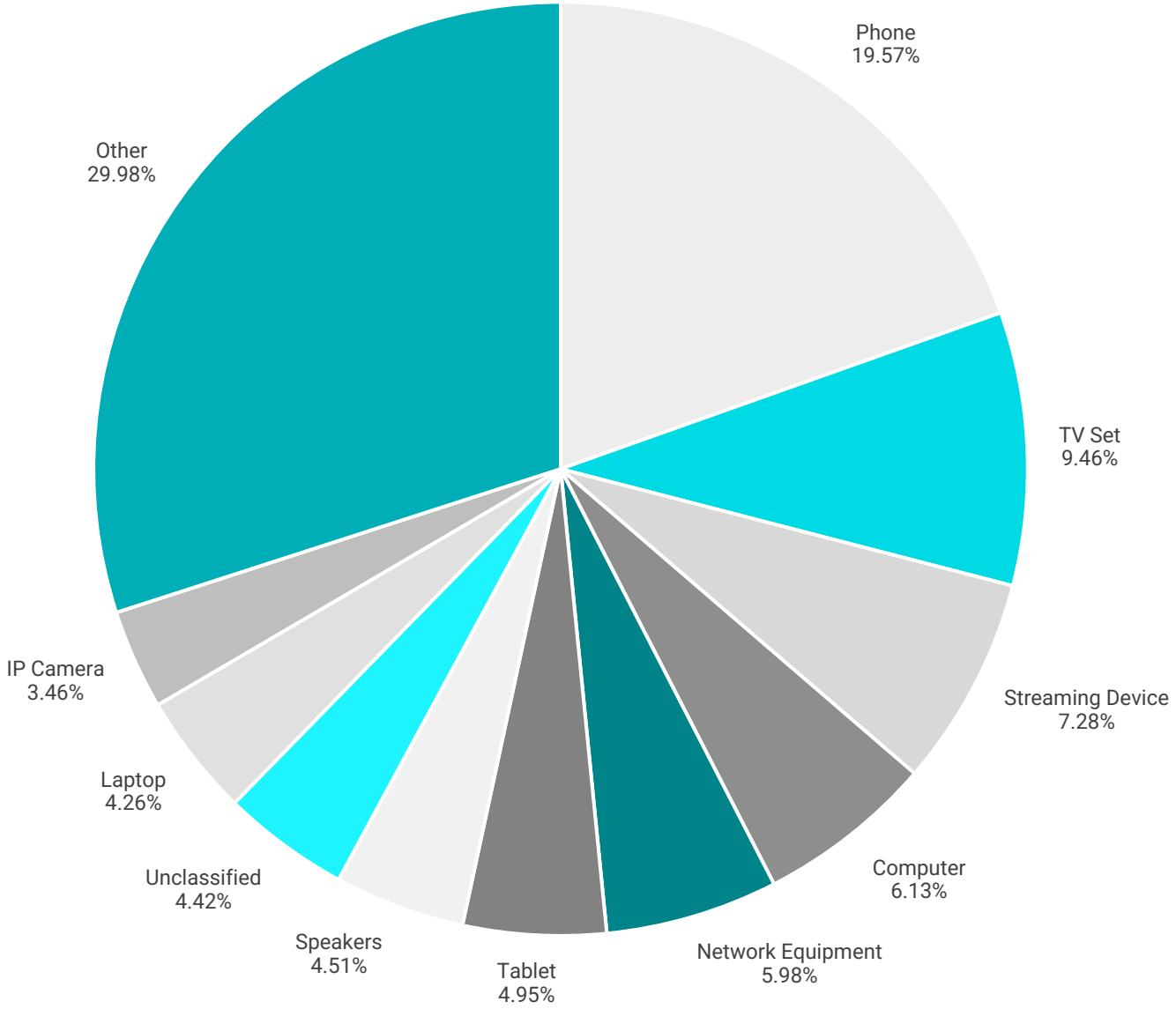
OTHERS

The shadow IoT: unseen, unnamed, but with a heartbeat and an IP address - from smart treadmills to kitchen toasters.

THE SMART HOME BUILDING BLOCKS

The connected home of 2025 is a dense ecosystem dominated by mobile phones (19.6%), which serve as the control hub for automation, entertainment and personal data. Smart TVs (9.5%) and streaming devices (7.3%) highlight how connectivity still revolves around screens, while traditional computers and laptops (10.3% combined) have shifted from the center of the network to become just another layer.

Nearly 30% of devices fall under “Other,” a mix of smart plugs, sensors, appliances, and unseen infrastructure that expands the household’s digital footprint. Along with network equipment, tablets, and speakers, the modern home increasingly resembles a small enterprise - always online, highly interdependent, and reliant on robust, network-level protection.



HIGH-TECH DING-DONG-DITCH

We analysed 13 billion security events targeting routers to understand the threat dynamics of the Internet, from the moment you plug a new router into the WAN connection provided by your Internet Service Provider.

More than 93% of the intercepts of our **Network Attack Defense** technology in 2025 are port scans - HighPorts and generic scanning. This shows the Internet never sleeps – it's constantly poking every exposed IP, over and over. It's not targeted malice so much as ambient hostility in the form of bots sweeping the net for open doors. The sheer scale shows how networks swim in a sea of low-skill, high-volume reconnaissance.

TOP ATTACKS

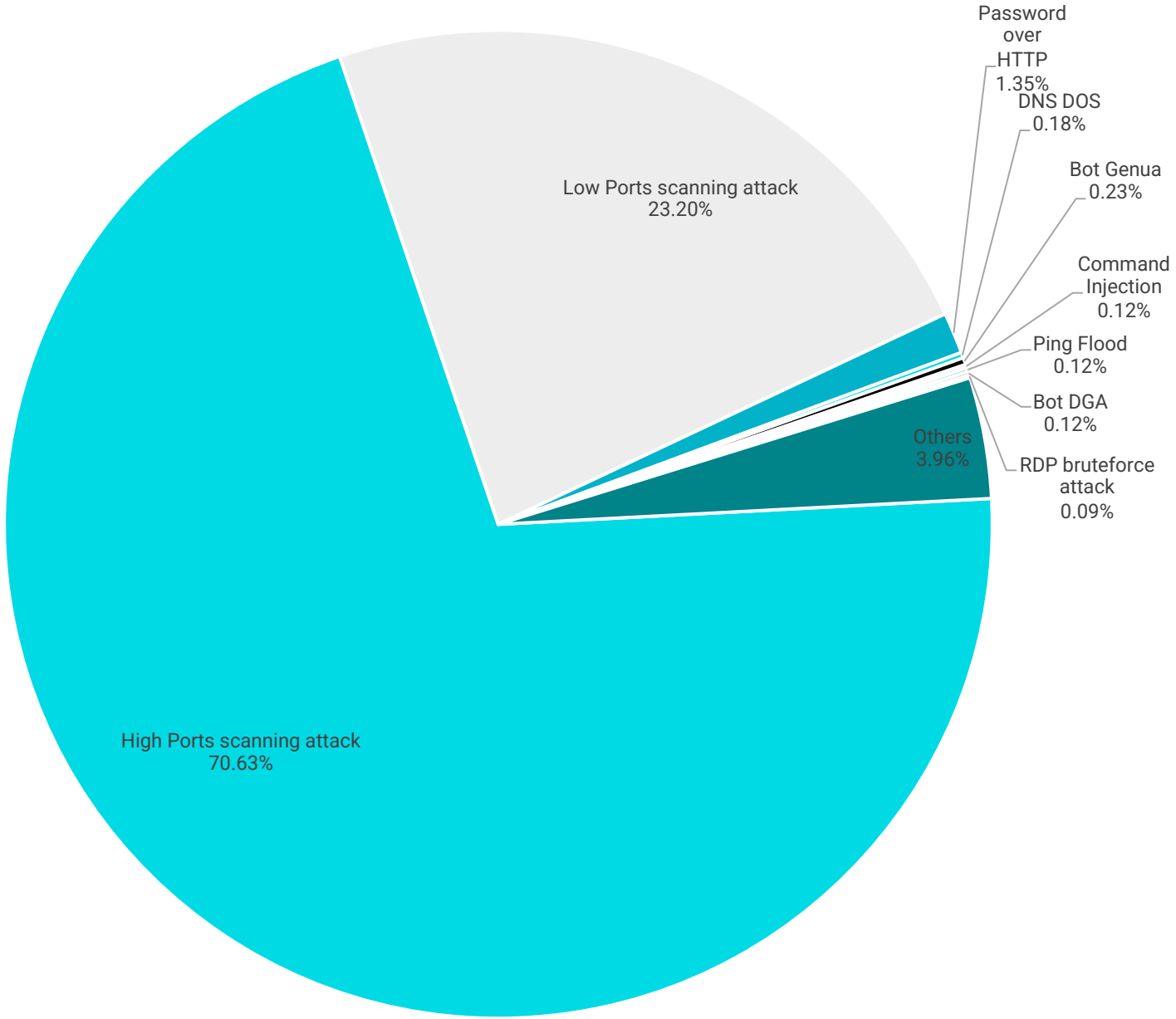
Password sending over HTTP (1.35%) still showing up means some devices or services are sending credentials unencrypted. HTTP hasn't been completely phased out in 2025.

DoS and PingFlood traffic represents more noise from infected IoT devices testing their DDoS capabilities.

The presence of DGA bots shows that compromised devices are still phoning home with algorithmically generated domain names.

Bot.Genua covers a wide range of RCE attacks, including OpenDreamBox, Dell KACE, and HooToo TripMate, as well as several well-known vulnerabilities such as CVE-2017-5174, CVE-2019-2725, CVE-2018-17173, and CVE-2014-8361.

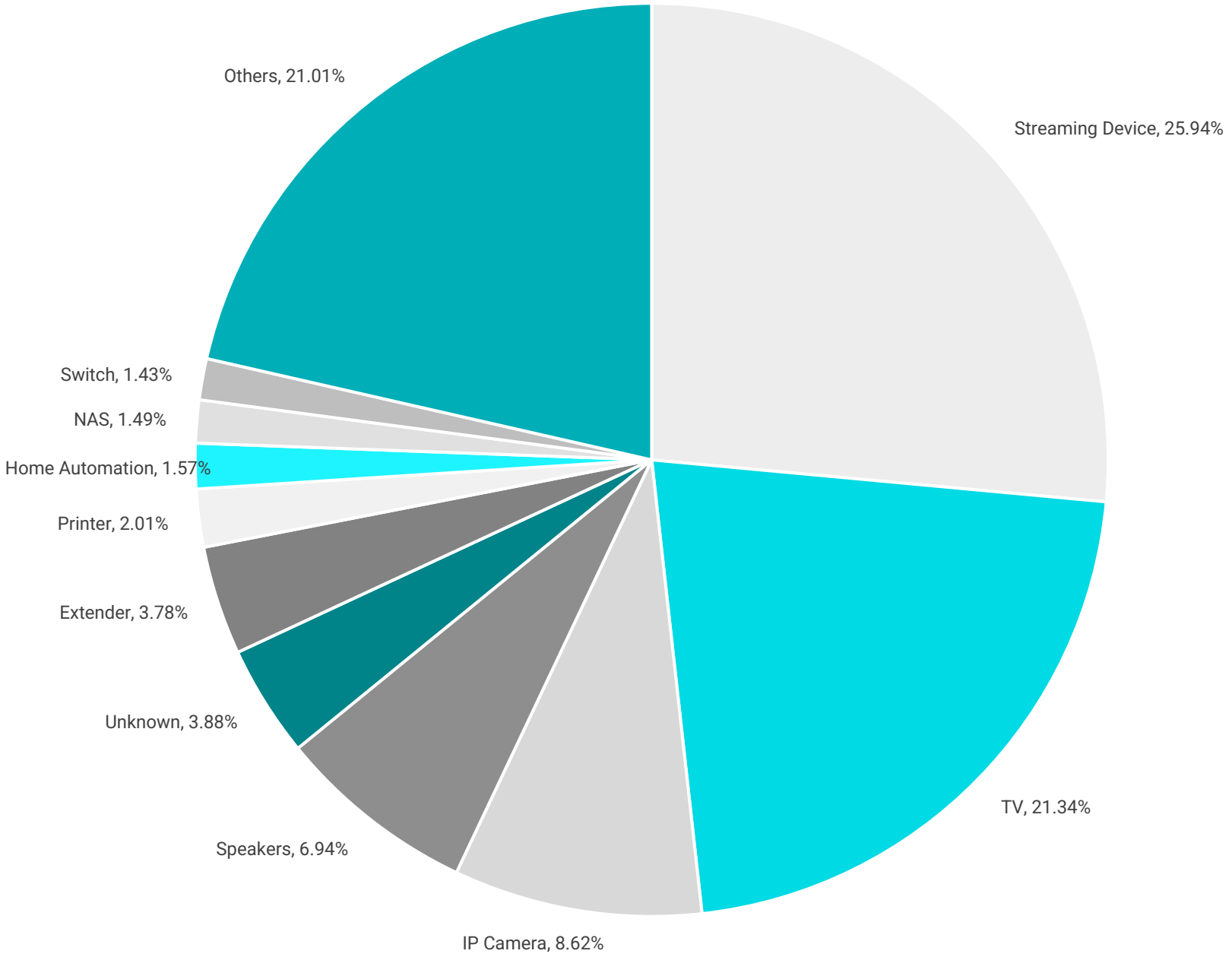
Though a tiny fraction, Command injections hint that attackers are still aiming at poorly sanitized web interfaces on IoT devices.



TOP VULNERABLE DEVICES

The distribution of vulnerable IoT devices paints a different picture of the modern smart home. Streaming devices now dominate, accounting for more than a quarter of all detected vulnerabilities, followed by smart TVs and IP cameras. Together, entertainment and surveillance gear represent over half of all exposed devices – yet another sign of how easily everyday consumer electronics can become security liabilities.

Printers, extenders, and network-attached storage systems also feature prominently, bridging the gap between leisure and infrastructure. These categories have been abused in large-scale malware campaigns such as BADBOX, which turn ordinary smart home gadgets into coordinated botnets that target networks far beyond the living room.



BADBOX - FACTORY-INFECTED DEVICES

The biggest threats to smart homes often start long before they get deployed on the household network. In June, the FBI warned streaming device owners about a new threat targeting their living rooms. The BADBOX botnet, now spanning more than a million Android-based and IoT devices worldwide, thrives on cheap, uncertified hardware sold online under obscure brands. Many of these devices - streaming boxes and projectors - arrive with malicious firmware already installed, silently enlisting their buyers into a network that launders traffic, commits ad fraud, and supports other criminal operations.

Once active, BadBOX turns compromised gadgets into residential proxies, allowing attackers to disguise their origin and push secondary payloads. The infections stretch across more than 220 regions, with the highest concentration in markets where low-cost imports dominate. Investigators have traced the operation to coordinated groups in China, where rebranded devices share identical backdoors and connect to the same control infrastructure. Industry efforts led by Google and law enforcement have disrupted portions of the network, but BadBOX 2.0's modular architecture and constant reemergence highlight how consumer electronics can become industrial-scale botnets. The case demonstrates that in the IoT world, compromise can be an unboxing experience.

SMART TV SETS

THE AGING TECH OF THE LIVING ROOM

Smart TVs account for 21.34% of all vulnerable IoT devices in our dataset. That's a near-perfect storm of risk: complex software stacks, long lifespans, and dismal update cycles. Most households keep TVs for five to eight years – far longer than manufacturers release security patches. Once vendor support ends, the device remains online, unpatched, and fully integrated into the home network.

Modern smart TVs are effectively full-fledged Android or Linux systems. They run app stores, browser engines, and third-party SDKs for streaming, advertising, and voice recognition. Each layer adds code complexity and expand the attack surface.

Read more on our research on smart TVs

SMART PLUGS

THE SILENT VICTIMS OF THE MODERN SMARTHOME

Smart plugs are cheap, ubiquitous, and often forgotten once installed. Their firmware is rarely updated, yet they're always online, serving as easy botnet recruits or network footholds. In 2025, the surge in smart energy automation and remote-controlled outlets drew renewed attention from attackers.

Throughout the year, several severe vulnerabilities in smart plugs have forced vendors to release emergency updates for entire product lineups. (1), (2)

NAS DEVICES

DATA GOLDMINES UNDER SIEGE

With cloud fatigue pushing consumers toward local storage, NAS boxes have become prized ransomware targets.

QNAP's Photo Station RCE (CVE-2024-27130) and Synology's DSM command-injection flaws were re-used in multiple ransomware campaigns. Groups such as Qilin and RA Group automated exploitation using Shodan to scan for exposed devices, encrypt data locally, and exfiltrate credentials to offshore servers.

A resurgence of Deadbolt ransomware variants targeted NAS owners directly via the device's public-facing interface, demanding Bitcoin payments in exchange for decryption keys. 'NAS-as-proxy' botnets appeared in parallel, leveraging compromised units to anonymize traffic for other cybercrime operations.

TOP CVES IN FIRMWARE

CVE	Description / Root Cause	Severity / Impact	Affected Component
CVE-2025-37803	Buffer size overflow in Linux kernel udmabuf_create() due to casting mismatch (size_limit_mb handling)	CVSS 3.1 = **7.8 (High)**	Many Linux kernel versions prior to patched versions (Debian, Ubuntu, Red Hat variants)
CVE-2025-37838	Use-after-free (UAF) in Linux kernel's HSI ssi_protocol driver due to race between workqueue and module removal	CVSS 3.1 = **7.8 (High)**	Kernel versions 6.7 up to <6.12.24, also earlier <6.1.135 etc.
CVE-2025-21751	In Linux kernel net/mlx5: error flow mis-handling in "matcher disconnect" path (HWS)	CVSS 3.1 = **7.8 (High)**	Affects mlx5 kernel driver (network interface) in vulnerable kernel versions used by distributions supporting that driver

A PREDILECTION FOR FRESH KERNEL CVES

Modern attacks prioritize the Linux kernel – the universal denominator across IoT ecosystems, from NAS units to cameras. These devices often run with minimal patching and exposed services. The spike in 2025-dated CVEs doesn't necessarily mean attackers are chasing novelty; it reflects that many IoT vendors ship firmware based on kernel trees that inherited vulnerabilities from upstream without integrating the corresponding fixes.

New CVEs are easier to weaponize at scale. Proof-of-concept code is published quickly, sometimes before vendors issue patches, which gives attackers a guaranteed window of opportunity. Older one, like those from 2023, are now broadly mitigated by firmware updates, network filtering, or attacker fatigue - they've simply burned out their return on investment.

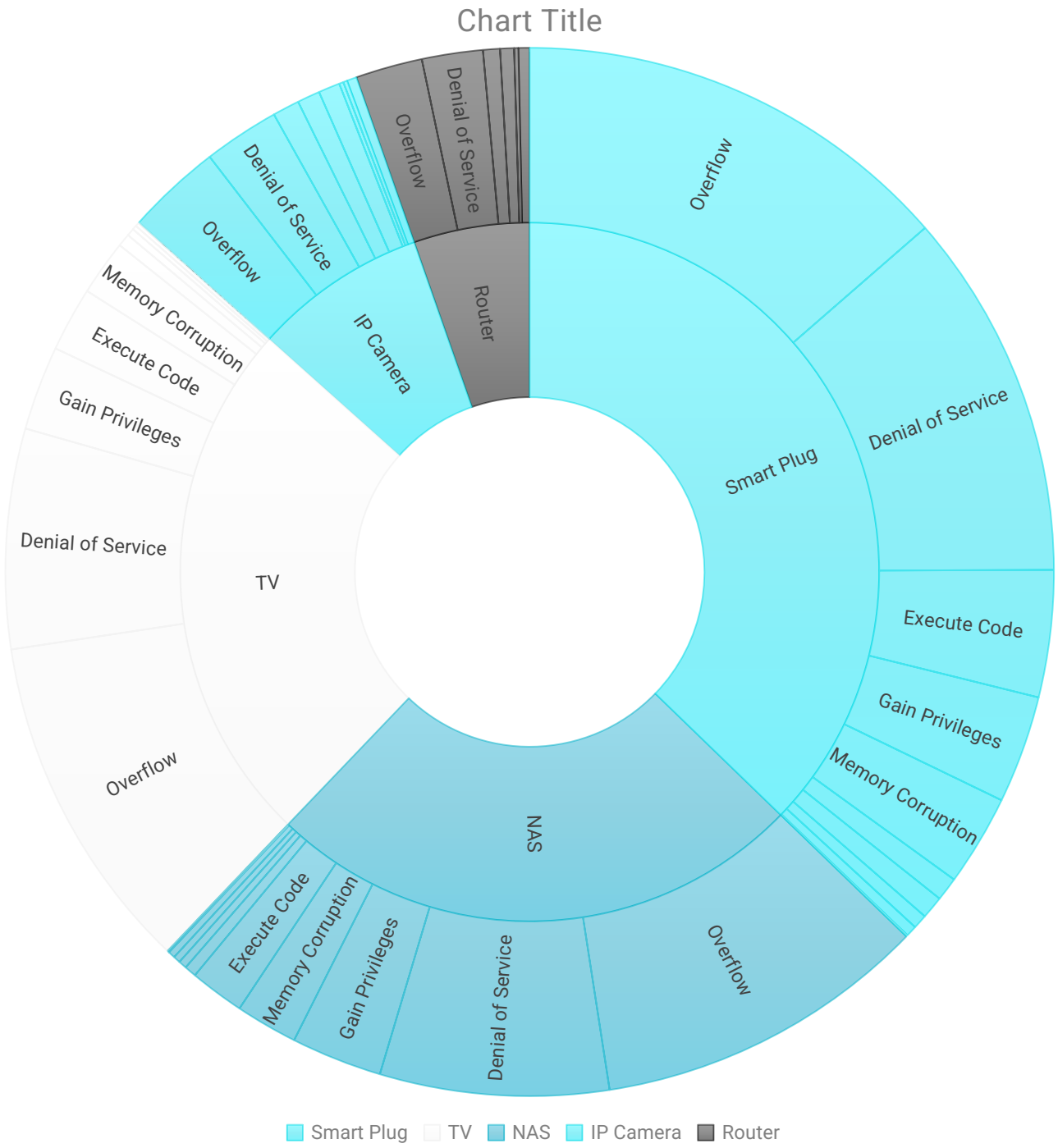
Modern exploit kits evolve automatically, refreshing their payload lists as new kernel flaws emerge. This ensures constant testing for unpatched targets. Weaponizing fresh CVEs is not about sophistication but about churn - staying one patch cycle ahead of manufacturers still stuck several years behind.

DEVICES BY VULNERABILITY TYPE

IoT insecurity stems from simplicity and scale. Overflow and DoS dominate across all device types, indicating poor memory safety and insufficient validation.

Devices meant to simplify life, like smart plugs, end up as the easiest entry points, while data-heavy appliances like NAS units become the most valuable targets.

TVs, NAS, and smart plugs together form the bulk of the modern IoT attack surface: complex, under-patched, and functionally essential, but often defenceless.

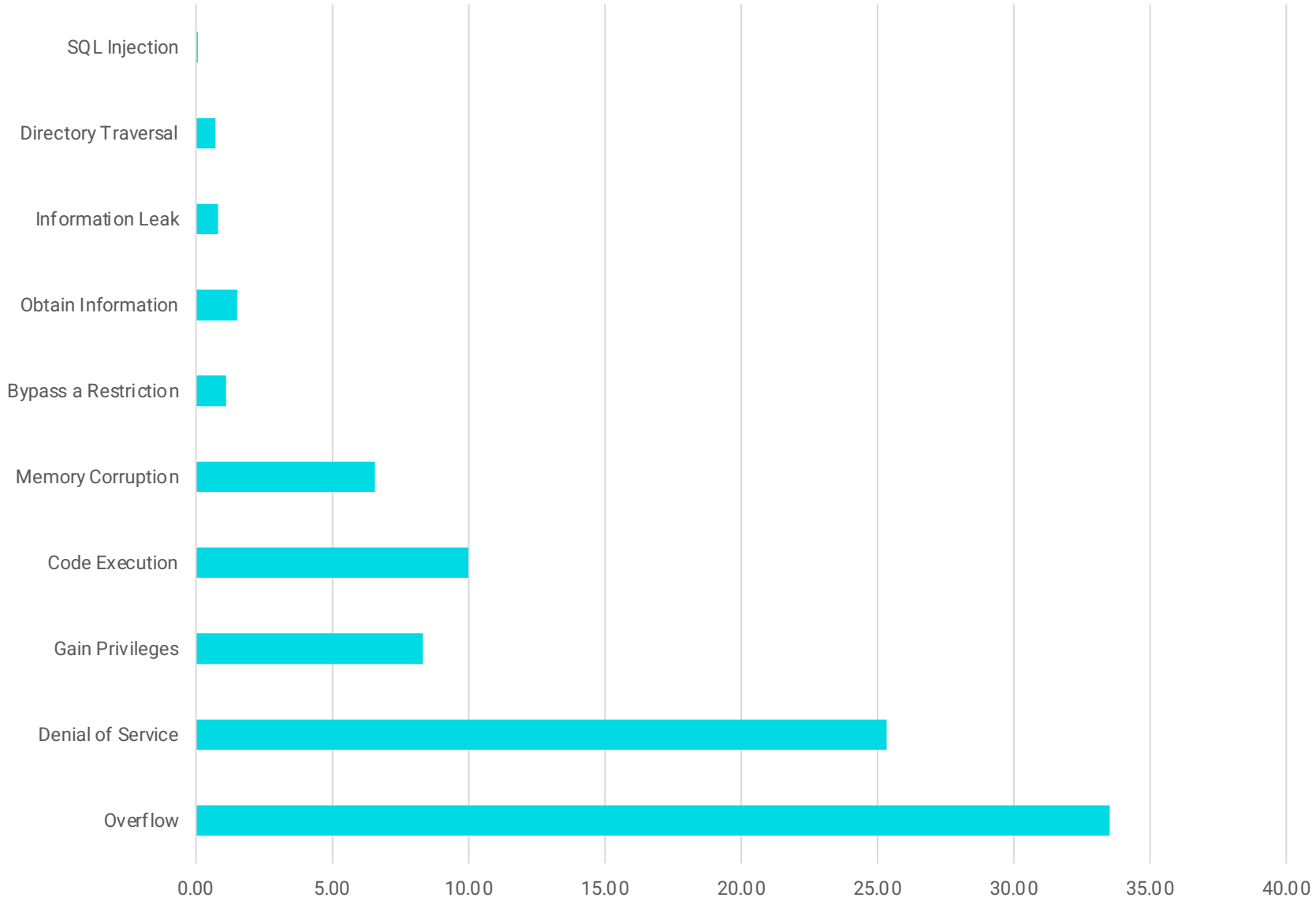


VULNERABILITIES BY TARGETED OUTCOME

The dominance of overflow and denial-of-service vulnerabilities shows attackers still favor disrupting device stability or exploiting basic memory flaws over complex logic bugs.

Privilege escalation and code execution issues are fewer but more impactful as they allow full control of compromised devices. The remaining categories - information disclosure, traversal, and injection - reflect persistent but narrower attack surfaces.

These results highlight uneven security maturity across IoT ecosystems, where device complexity often correlates with vulnerability exposure. In short, the smarter the device, the more creative the ways it can break.



OBSERVATIONS AND TRENDS

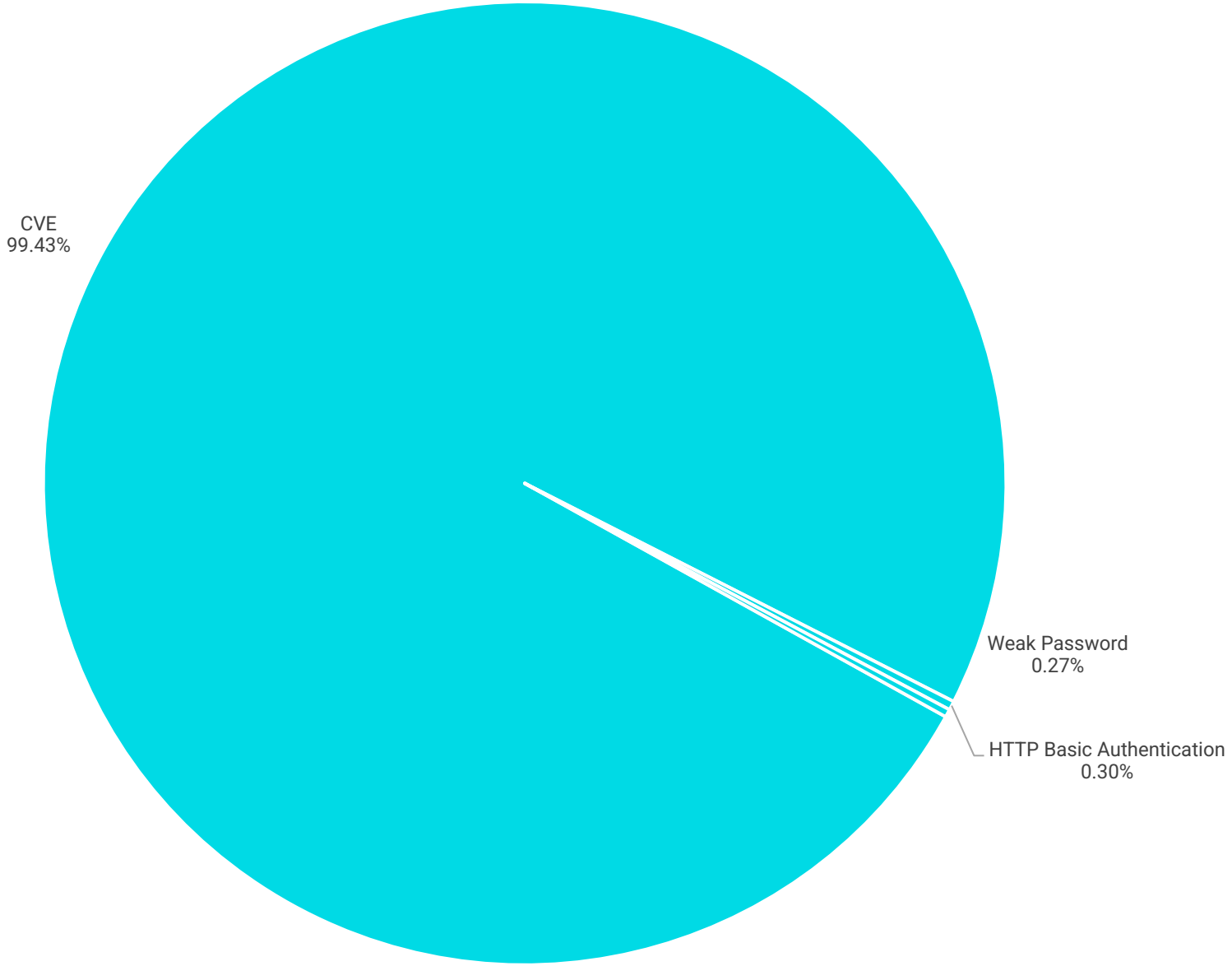
Streaming devices, smart TVs, and IP cameras now sit at the top of the vulnerability pyramid, collectively representing more than half of all CVE-class issues detected in smart homes. Most flaws still fall into the overflow and denial-of-service categories, exposing these devices to system crashes and remote code execution attempts. Streaming boxes - often built on generic Android forks - inherit the same insecure firmware design that powers millions of low-cost IoT gadgets, making them prime targets for large-scale malware like BADBOX.

Smart TVs follow closely, their rich feature sets and long lifespans leaving plenty of room for unpatched code and abandoned SDKs. IP cameras complete the trio, combining network exposure with weak authentication and a predilection for exposure over the Internet, effectively serving as ready-made backdoors into home networks. Together, these devices show how entertainment and surveillance gear have become the soft underbelly of the connected household - powerful, persistent, and largely unmaintained.

VULNERABILITY TYPES AND RISK VALUES

Known (and fixed) CVEs represent the vast majority of IT vulnerabilities. Only a fraction of attacks leverage weak passwords or plaintext authentication.

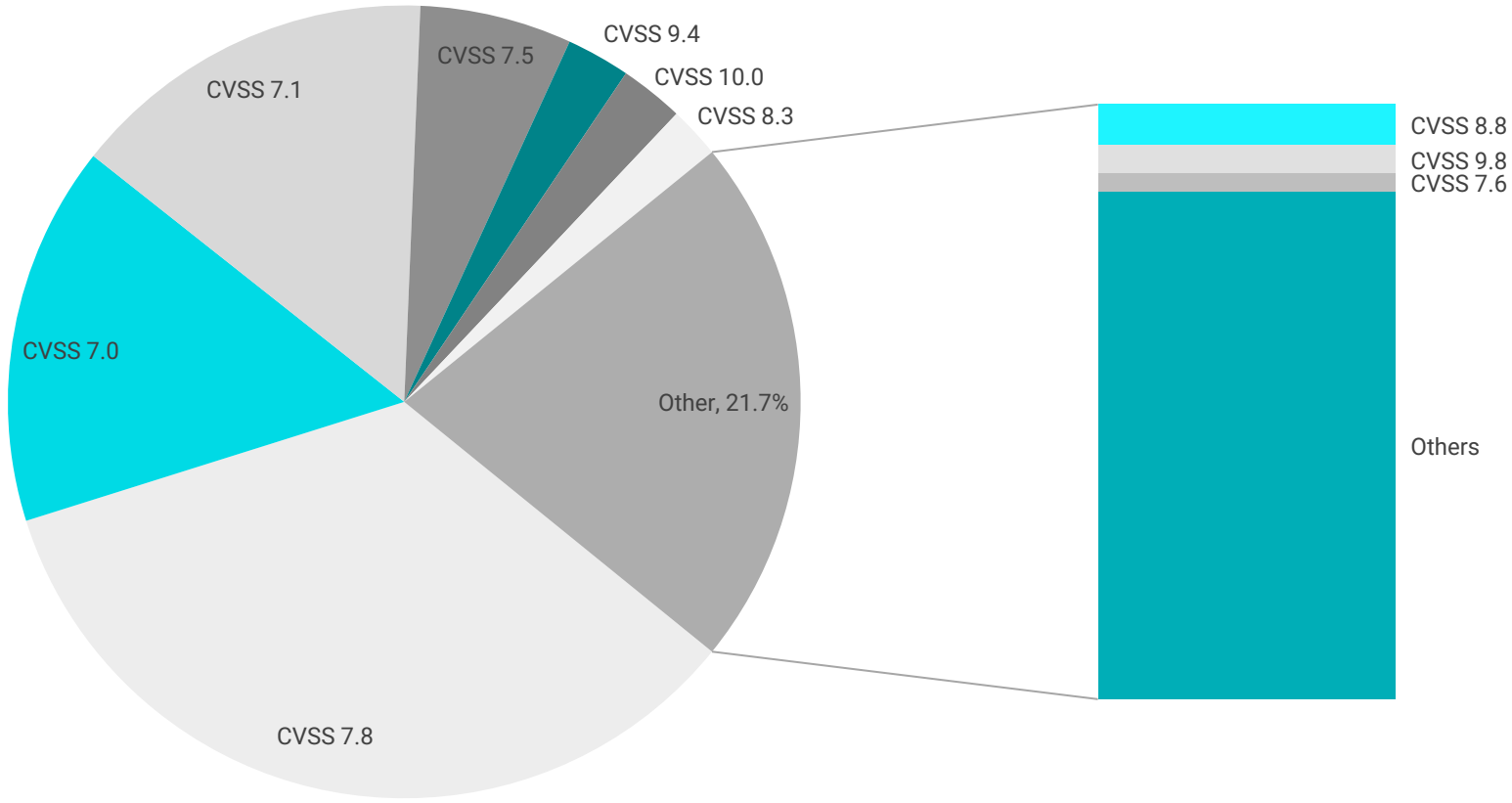
Looking closer at the CVE distribution, we see that most vulnerabilities are HIGH severity (CVSS 7.8) and depict a very common IoT baseline flaw.



VULNERABILITY RISK VALUES

The distribution of CVSS scores attests to a persistent pattern in IoT security: most vulnerabilities fall within the High severity range (7.0 -7.8). These vulnerabilities, while not immediately catastrophic, represent systemic weaknesses in firmware and network-facing services that remain exploitable over long periods, often due to infrequent patching or fully discontinued.

The CRITICAL severity segment (9.0 - 10.0) accounts for a smaller proportion of the total but reflects vulnerabilities that allow complete device compromise, such as remote code execution or privilege escalation.



A GUIDE TO IOT CVE OUTCOMES

CVSS SCORE*	% OF TOTAL	NOTES
7.0	15.5%	HIGH severity, remotely reachable issues with limited mitigation
7.1	15%	HIGH severity, recurring authentication and configuration flaws
7.5	6.2%	HIGH severity; persistent network-facing vulnerabilities (widely spread across firmware CVEs)
7.6	0.7%	HIGH severity, often describing authentication bypass techniques or weak credential handling
7.8	34.3%	HIGH severity; very common IoT baseline flaw
8.3	2.1%	HIGH severity; typically describing improper access control vulnerabilities
8.8	1.5%	CRITICAL severity, usually describing privilege escalation vulnerabilities
9.4	2.6%	CRITICAL severity; usually describing unauthenticated remote code execution & full compromise
9.8	1%	CRITICAL severity; usually describing privilege escalation and lateral movement risks
10	2.6%	CRITICAL severity; total device takeover scenarios

*CVSS Scores are computed using CVSS 3.1, or Common Vulnerability Scoring System version 3.1, a standardized framework used to assess and communicate the severity of security vulnerabilities in software and systems.

LOOKING AHEAD AT 2026

1 Router Botnets Go Industrial

IoT botnets are expected to continue their evolution, with router-based networks expanding beyond consumer environments into the infrastructure of small and medium-sized businesses. As residential and office networks increasingly share similar hardware and connectivity models, attackers will exploit these overlapping ecosystems to amplify distributed denial-of-service (DDoS) capabilities. Future botnets may integrate a diverse mix of routers, EV chargers, smart inverters, and industrial controllers, significantly broadening the available attack surface.

This convergence marks a shift from traditional consumer-grade threats toward hybrid IoT botnets with the bandwidth and reach to disrupt enterprise operations and critical services. As a result, network segmentation, firmware integrity, and automated detection of anomalous outbound traffic will become essential for both consumers and ISPs seeking to contain these large-scale, cross-domain attacks.

2 Firmware Supply Chain Becomes Ground Zero

In 2026, attackers are likely to focus further up the supply chain, targeting firmware components and development kits used across entire product ecosystems. Vulnerabilities in shared libraries, SDKs, or update mechanisms can silently propagate through multiple brands and device categories, creating systemic exposure. Compromising firmware signing infrastructure or over-the-air (OTA) update services will offer attackers a scalable, long-term foothold that is difficult to detect and nearly impossible to remediate in the field.

To address this, manufacturers and integrators will be forced to implement verifiable software bills of materials (SBOMs) and continuous integrity verification across build pipelines. Greater transparency and cryptographic validation of update mechanisms will become a baseline expectation in procurement and compliance frameworks, reinforcing trust in IoT ecosystems from production to deployment.

3 Privacy Erosion and Data Oversharing

IoT ecosystems continue to generate unprecedented amounts of behavioural, environmental, and biometric data. Many vendors collect this information to train algorithms or refine services, often with minimal transparency. As devices become more context-aware, the boundary between legitimate telemetry and intrusive surveillance will blur even further, creating growing concern among regulators and consumers alike.

In 2026, data protection authorities are expected to strengthen oversight of how IoT vendors store, process, and share user information. Compliance with privacy laws such as GDPR and CCPA will require manufacturers to implement privacy-by-design architectures and clear data retention policies. Users will increasingly demand local data processing and explicit consent mechanisms, reshaping how connected products handle sensitive information.

HOW TO STAY SAFE IN 2026

Most breaches in smart homes happen because of outdated, misconfigured, or abandoned devices. Security demands visibility and continuous device monitoring.

- Know what's connected. Keep an updated inventory of all IoT and networked devices at home or work. Disable the ones you no longer use.
- Replace legacy hardware. Devices that are no longer supported or updated are permanent liabilities - swap them for models that receive regular security patches.
- Segment your network. Keep smart plugs, cameras and appliances on a separate network, away from personal devices
- Patch devices as soon as a new firmware version becomes available.
- Use routers or gateways with built-in security.
- Avoid exposing LAN devices to the Internet unless necessary

NETGEAR® ARMOR™ | POWERED BY Bitdefender®

A MULTI-LAYERED APPROACH TO HOME SECURITY

The data is clear: the modern household faces continuous, automated cyber threats, averaging nearly 30 attacks every day. From smart TVs to doorbells, the devices that make life easier are now the very entry points attackers exploit. The need for built-in, network-level security is clearer than ever.

NETGEAR Armor™, powered by Bitdefender®, helps deliver that protection. Available through Nighthawk routers and Orbi Mesh WiFi systems, Armor helps to detect and block known and emerging threats, identify vulnerabilities, and strengthen privacy across network connected devices.

Together, NETGEAR and Bitdefender combine two trusted strengths: NETGEAR's long-standing leadership in connectivity performance and innovation, and Bitdefender's proven cybersecurity expertise and threat intelligence. The result is a connected home experience built on speed and strengthened by powerful security features, inspiring confidence in every connection.


Bitdefender
WWW.BITDEFENDER.COM/IOT