Bastille

THREAT REPORT

The State of Wireless Security in 2026

A 230× Rise in Annual Wireless CVEs Since 2010, 20x Faster Than Non-Wireless CVEs, Sustained by a Decade of 25%+ Yearly Growth

Principal Researcher:
Dr. Brett Walkenhorst
CTO, Bastille Networks Inc.

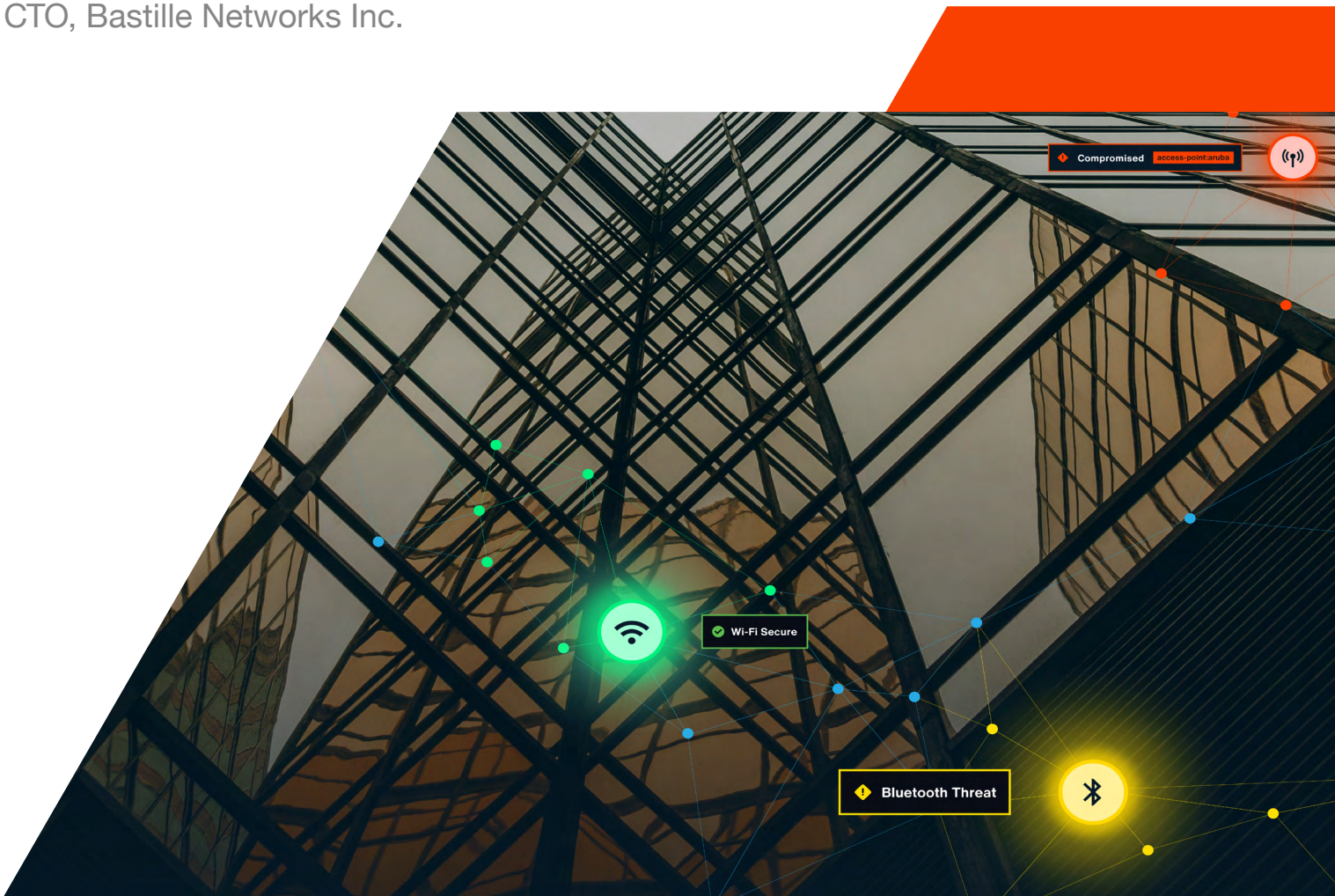

Table of Contents

Executive Summary

Wireless vulnerabilities have been expanding at an accelerating rate, materially increasing enterprise risk exposure across IT, operational technology, and embedded systems environments.

Over the past fifteen years, wireless CVEs have grown at a rate more than 20× faster than total CVE disclosures when indexed against 2010 baselines. Wireless vulnerabilities now account for nearly 2% of all reported CVEs annually, a notable share given that this single functional attack surface spans vendors, industries, and device categories.

In 2025, researchers disclosed 937 new wireless-related Common Vulnerabilities and Exposures (CVEs), an average of 2.5 per day. These represent a 27% increase over previously published wireless CVEs, bringing the cumulative total to 4,437.

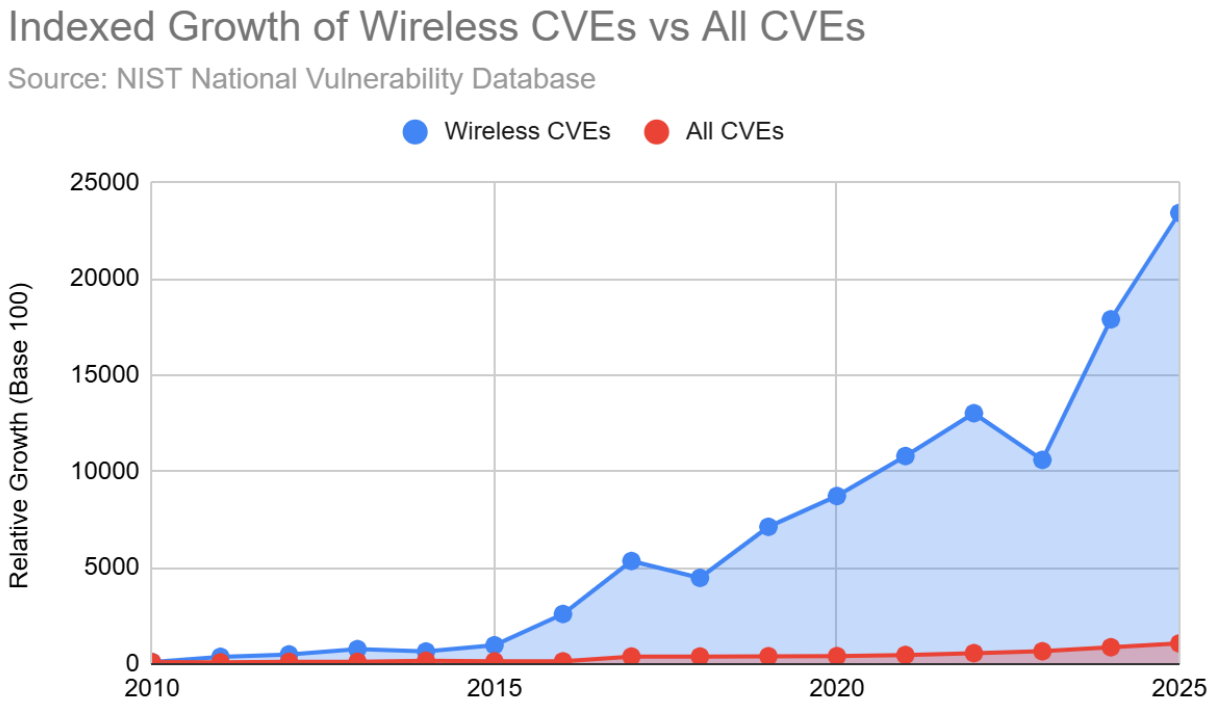

Figure 1 depicts the indexed growth of wireless CVEs vs. all CVEs from 2010 to 2025, with 2010 set to 100, demonstrating that wireless CVEs are growing at a rate 20x that of total CVEs.

The prior year showed similar momentum. In 2024, researchers disclosed 716 new wireless CVEs, representing approximately 26% cumulative growth. Year-over-year growth in new annual wireless CVEs was 30%. Two consecutive years of 25%+ base expansion demonstrate sustained acceleration rather than anomaly. The last two years saw a combined 60% increaserelative to the start of 2024. Since 2014, the total number of wireless CVEs has doubled every 2-4 years.

Wireless Threat Growth 2010-2025

Source: NIST National Vulnerability Database

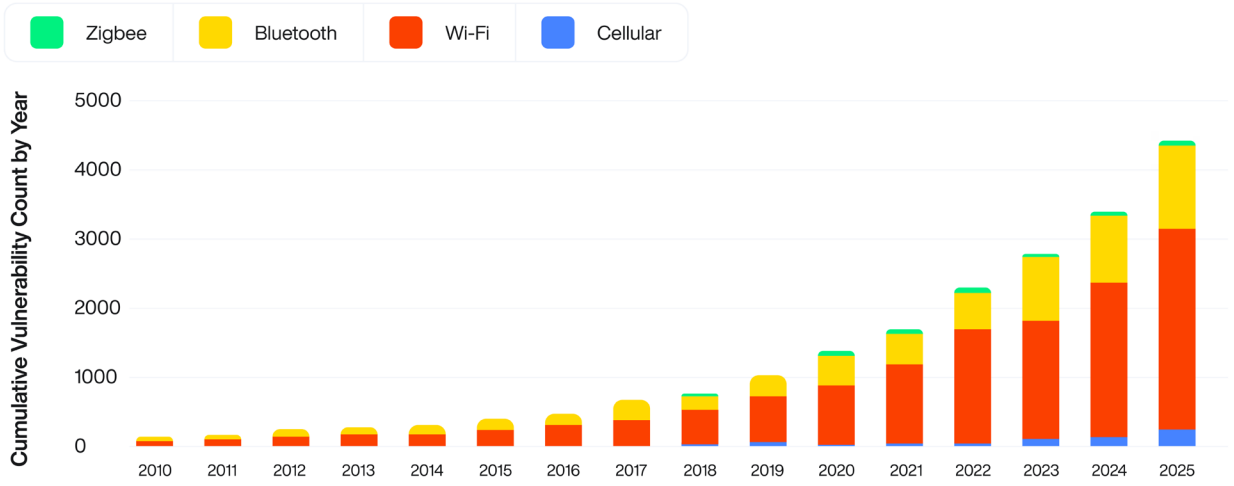

Figure 2 depicts the exponential growth in wireless CVEs over the past 15 years by protocol, covering Wi-Fi, Cellular, Bluetooth, and Zigbee.

This increase occurs amid a broader surge in vulnerabilities. Industry forecasts project that total annual CVE disclosures across all technologies will exceed 50,000, reflecting unprecedented reporting velocity across software, firmware, infrastructure, and embedded systems. Wireless vulnerabilities represent a subset of this expansion, but one with disproportionate operational implications.

The trajectory shows no plateau. If current growth persists, annual wireless CVE disclosures will exceed 1,500 per year within the next several years.

For enterprise leaders, this trend signals a structural shift in risk. Wireless CVEs increasingly impact operational continuity, regulatory posture, and incident response complexity as Wi-Fi, Bluetooth, Zigbee, LTE, and 5G become foundational to business operations. Traditional vulnerability management models that rely on asset inventories, patch tracking, and IP-based scanning do not fully address wireless exposure.

The data underscores a clear requirement: wireless risk management must move beyond static inventories and periodic assessments toward continuous visibility into wireless activity.

1. CVE Analysis

1.1 Scope and Context of Wireless CVE Growth

Wireless CVEs encompass vulnerabilities affecting systems that rely on radio-frequency communications rather than on wired connectivity or application-layer network traffic alone. These vulnerabilities often persist longer and carry a broader impact than traditional IT CVEs.

Several characteristics distinguish wireless CVEs from conventional software vulnerabilities:

- Exposure frequently exists independent of IP connectivity
- Affected devices often operate outside centralized security management
- Vulnerabilities commonly apply at the protocol or chipset level, impacting multiple vendors simultaneously
- Attackers can leverage these vulnerable devices to launch further wireless attacks
- Patching is inconsistent: some devices or protocol implementations never receive patches, and some devices are not patchable, such as IoT or SCADA devices.

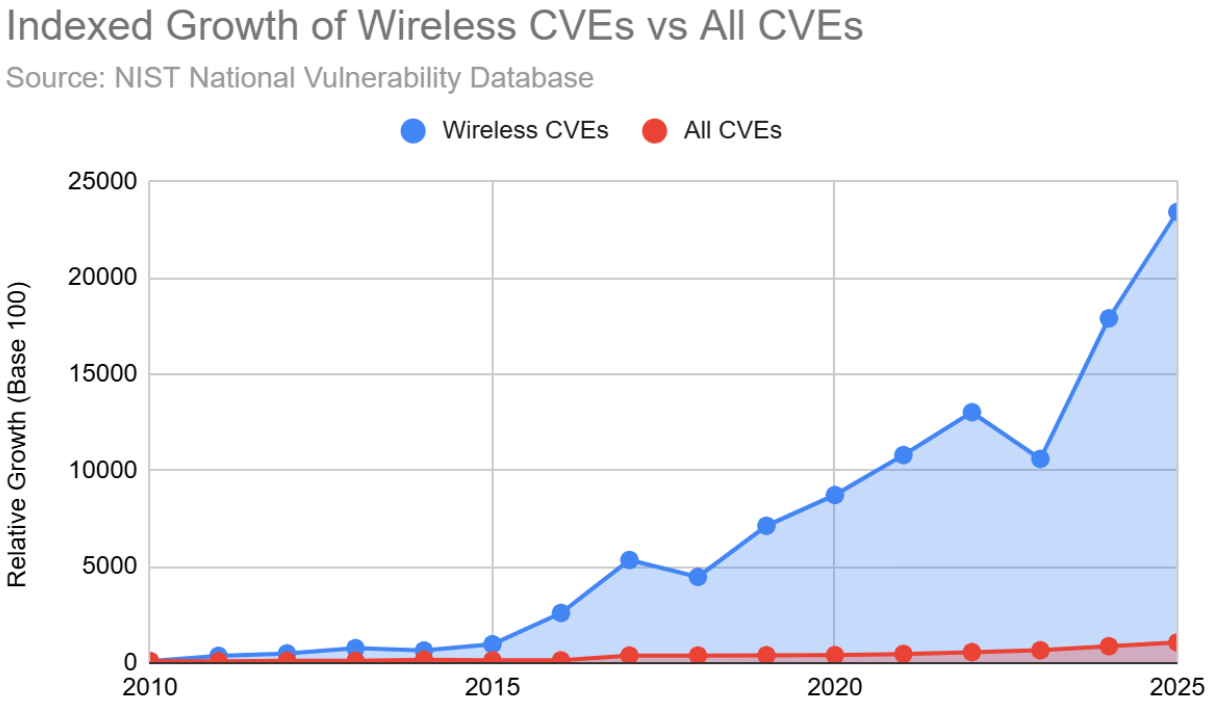

Figure 3 depicts the indexed growth of wireless CVEs vs. all CVEs from 2010 to 2025, with 2010 set to 100, demonstrating that wireless CVEs are growing at a rate 20x that of total CVEs.

Traditional vulnerability management assumes that assets are known, addressable, and centrally managed. Wireless environments violate these assumptions. As a result, cumulative growth in wireless CVEs increasingly translates into long-term exposure rather than short-term remediation efforts.

Over the past 15 years, the number of annual wireless vulnerabilities has grown by more than 230×, from 4 in 2010 to 932 in 2025. When indexed against 2010 baselines, wireless vulnerabilities have grown at a rate more than 20× faster than overall CVE disclosures. Since 2016, wireless flaws have entered a sustained acceleration phase, with two consecutive years exceeding 25% cumulative base expansion (2024 and 2025). Except for 2023, which saw 18% growth, the last 10 years have seen annual growth rates for wireless CVEs exceeding 25%, with a peak growth rate of 56% in 2017. Wireless vulnerabilities now account for nearly 2% of all reported vulnerabilities annually.

The 937 new wireless-related CVEs in 2025 represent an average of 2.5 new CVEs per day. These represent a 27% increase over previously published wireless CVEs, bringing the cumulative total to 4,437. In 2024, the number of new wireless CVEs was 716, representing a 26% increase in the cumulative total. The last two years saw a combined 60% increase relative to the start of 2024. The total number of wireless CVEs has doubled every 2-4 years since 2014.

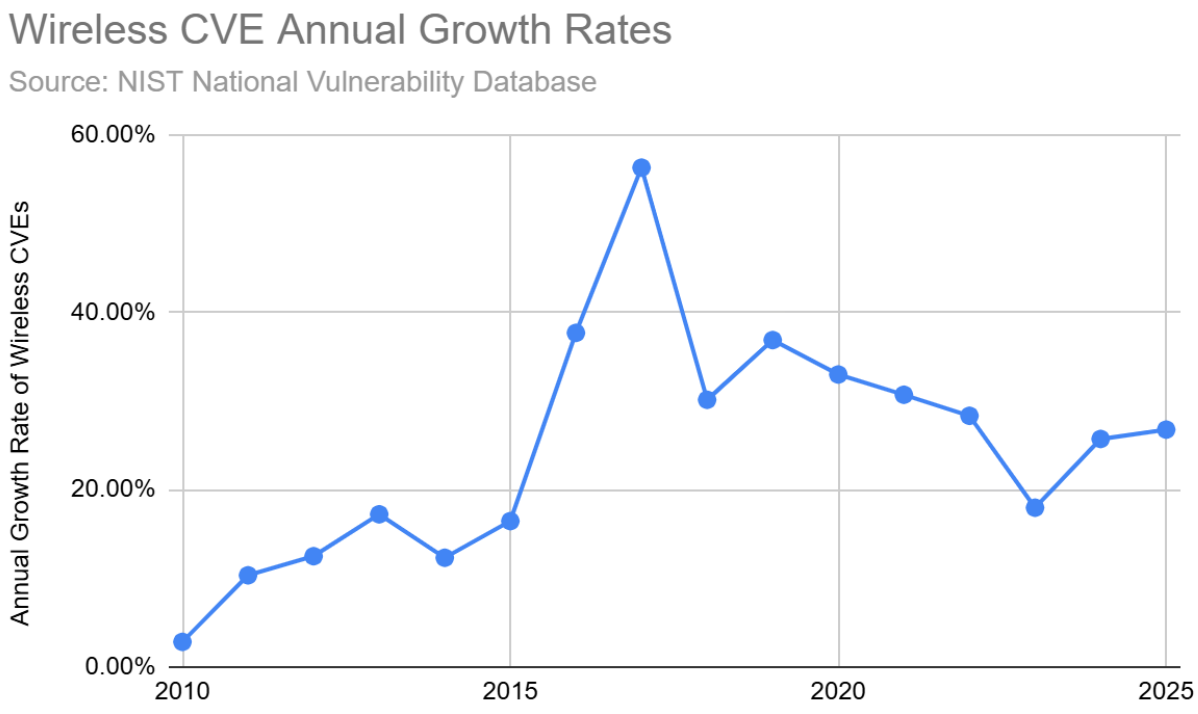

Figure 4 shows the annual growth rate of wireless CVEs. Except for 2023 at 18%, growth rates have consistently exceeded 25% from 2016 through 2025.

Wi-Fi and Bluetooth drive most of this growth, while cellular and IoT protocols steadily expand the attack surface. The data shows not just rising volume but also the structural expansion of the wireless risk domain.

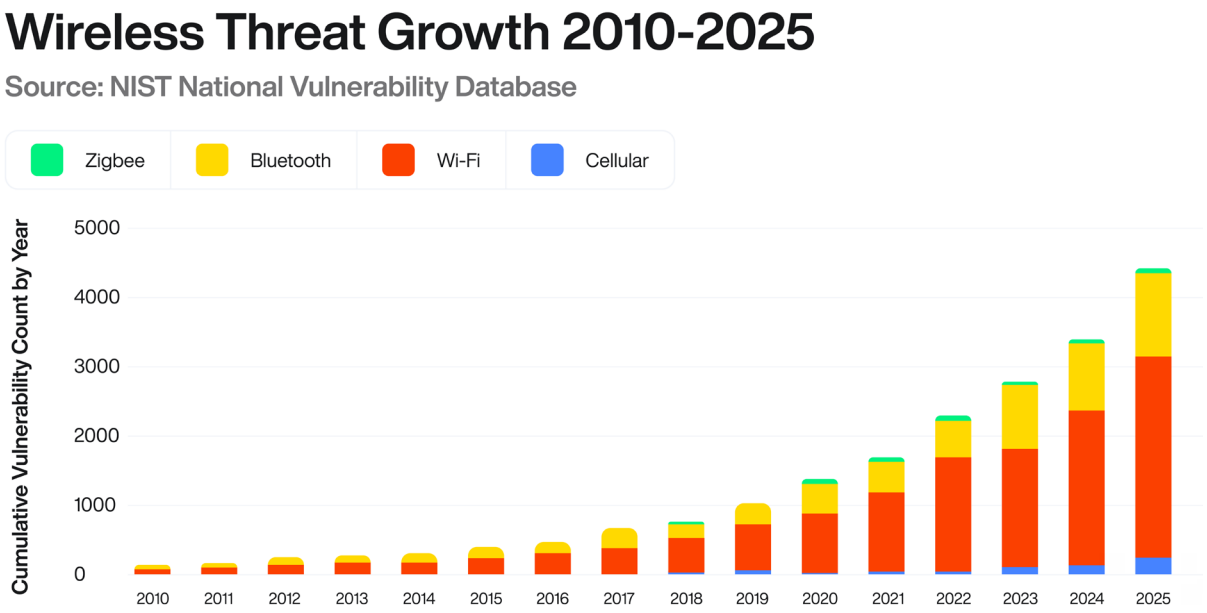

Figure 5 depicts the exponential growth in wireless CVEs over the past 15 years by protocol, covering Wi-Fi, Cellular, Bluetooth, and Zigbee.

Figure 5 shows a typical exponential curve:

- Modest growth pre-2015
- Rapid acceleration post-2016
- Steep slope from 2020 onward
- 2023–2025 showing the largest year-over-year increases

This trend does not indicate a plateau. If the trajectory continues, wireless CVEs will exceed 1,500 annually within a few years.

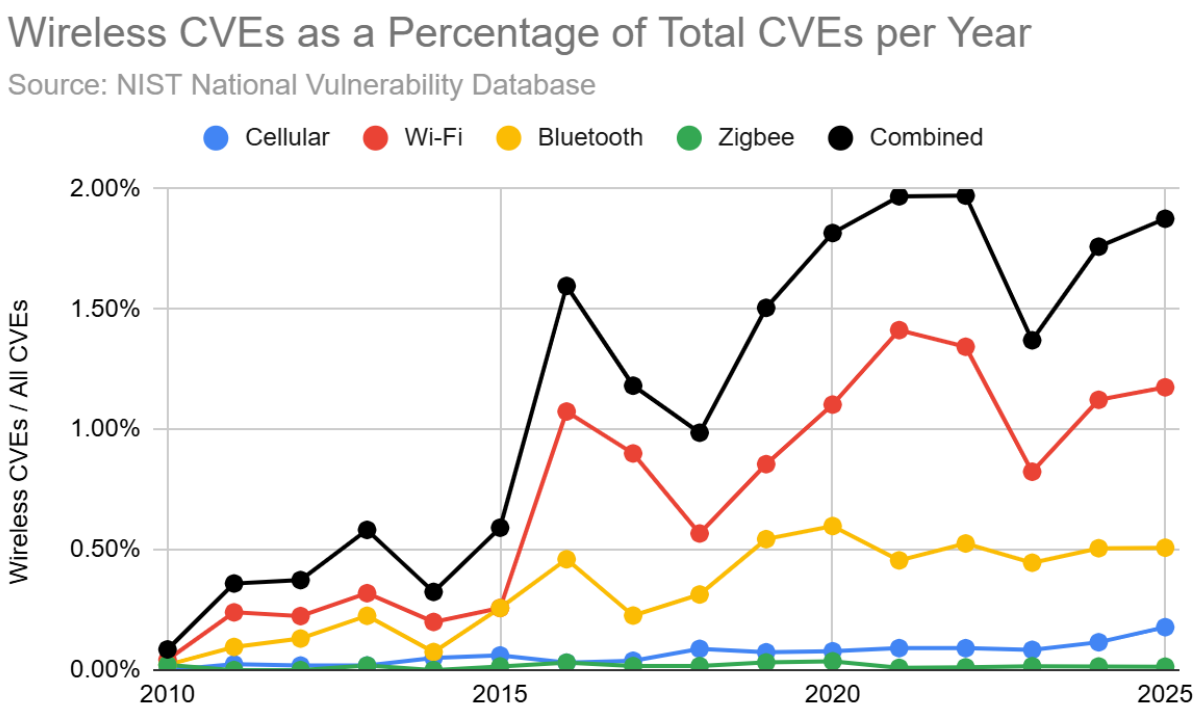

Figure 6 depicts the percentage of wireless CVEs over the past 15 years relative to the total number of CVEs per year, by protocol. The black line indicates the aggregate of all the other lines.

1.2 Wi-Fi Dominates the Wireless Risk Landscape

Wi-Fi is consistently the largest contributor to the wireless CVEs. It drives most of the cumulative growth curve. It explains most of the post-2016 spike. By 2025, Wi-Fi is likely to account for ~60%+ of wireless CVEs.

1.3 Bluetooth Is the #2 Driver, and More Vola-

Bluetooth has multiple surge years. There is a clear post-2016 acceleration. While it tracks slightly below Wi-Fi, it follows a similar trend. Because Bluetooth is ubiquitous across mobile, medical, automotive, and IoT, this growth is operationally significant.

1.4 Cellular CVEs Are Growing Quietly, and Likely Underestimated

Cellular counts remain lower in raw counts but show a steady increase over time. There is a gradually rising percentage share and a strong cumulative slope in Figure 1. Given 5G rollout,baseband complexity, and carrier firmware opacity, this category may be structurally underreported relative to actual exposure.

1.5 Zigbee Is Small, But Symbolically Important

Zigbee remains low in percentage terms. However, it reflects IoT protocol-level weaknesses, appears consistently year over year, and is representative of embedded/home-automation environments. Wireless risk is not limited to enterprise IT. It extends into OT and smart environments.

1.6 The Increasing Number of Wireless

Wireless now represents nearly 2% of all CVEs in 2025. That may sound small, but consider that wireless is one functional class of vulnerabilities. It cuts across vendors, industries, and device types, and often bypasses traditional perimeter controls. It thus represents a disproportionate operational risk relative to its percentage, especially because wireless flaws often enable remote attacks, bypass network segmentation, and target unmanaged devices.

1.7 The Wireless Attack Surface Is Outpacing Defensive Architecture

Traditional vulnerability management focuses on IP-addressable assets, scans servers and endpoints, and assumes patchable OS-level control.

Wireless vulnerabilities often affect firmware, drivers, embedded stacks, IoT devices, and baseband processors.

As wireless CVEs scale faster than total CVEs, the gap between Exposure Visibility and Exposure Management is widening.

2. Methodology

2.1 CVE Identification and Classification

This analysis reviewed publicly disclosed CVE records and identified wireless-related vulnerabilities based on their exploitation mechanisms and their reliance on RF communication. Analysis included CVEs when exploitation directly involved the following:

- Wi-Fi protocols, chipsets, firmware, drivers, or access point infrastructure
- Bluetooth protocol stacks, system-on-chip platforms, and device firmware
- Zigbee mesh networking implementations and trust models
- Cellular modem firmware and LTE or 5G protocol handling

Analysis excluded CVEs affecting applications or operating systems lacking a wireless component.

2.2 Temporal and Growth Analysis

Annual CVE counts used the disclosure year. Cumulative totals reflect all previously published wireless CVEs. Percentage growth represents year-over-year increases relative to the cumulative baseline at the beginning of each year.

2.3 Impact and Visibility Assessment

Analysis reviewed public reporting, vendor advisories, and national media coverage to identify high-impact wireless CVEs disclosed in 2025.

2.4 Methodological Limitations

This analysis relies on publicly disclosed CVEs and associated reporting. Some wireless vulnerabilities may remain undisclosed or described in limited detail due to proprietary considerations. Classification of hybrid vulnerabilities that span wireless and application layers may introduce ambiguity. These factors suggest that reported figures likely underrepresent total wireless exposure.

3. Drivers of Sustained 25% Growth in Wireless CVEs

Two consecutive years of approximately 25% expansion in the wireless CVE base reflect structural forces rather than short-term reporting fluctuation. The sustained growth rate results from both increasing disclosure volume and persistent exposure conditions that allow vulnerabilities to accumulate faster than mitigation can address them.

3.1 Drivers of Disclosure Volume

Broader vulnerability forecasting suggests that total CVE counts across all domains will exceed 50,000, indicating that wireless protocols are part of a pervasive acceleration in vulnerability discovery and reporting. Wireless adoption continues to expand across enterprise and operational environments. Wi-Fi and Bluetooth support workforce productivity, while Zigbee, LTE, and 5G enable building systems, industrial sensors, and mobile infrastructure. Increased deployment expands the attack surface and contributes to disclosure volume.

As use cases addressed by wireless protocols continue to expand, the wireless specifications and their implementations become increasingly complex. This increasing complexity, necessary to address new and creative use cases, introduces more and more vulnerabilities.

Security research has increasingly placed greater emphasis on wireless protocols, which historically received less scrutiny than traditional IT stacks.

3.2 Drivers of Persistent Exposure

Wireless vulnerabilities often remain relevant long after disclosure. Device longevity, certification requirements, and operational constraints delay or prevent patch adoption. In Zigbee and cellular deployments, remediation may depend on vendor firmware updates or compensating controls rather than direct fixes. These factors extend exposure windows and compound risk over time.

4. High-Profile Wireless CVEs in 2025

4.1 Bluetooth Vulnerabilities in Audio and Wearable Devices

Bluetooth vulnerabilities disclosed in 2025 affected millions of wireless headphones, earbuds, and wearables built on common Bluetooth chipsets. Public reporting described unauthorized connections without user interaction, extraction of cryptographic material, device impersonation, and potential audio eavesdropping. These disclosures received national media attention due to their scale and the limited remediation options available.

For example, WhisperPair (CVE-2025-36911) is a Bluetooth vulnerability that enables attackers to force vulnerable wireless audio accessories to pair without user interaction or physical access. Using any Bluetooth-capable device, attackers can initiate pairing for any device within range in seconds. Once paired, an attacker can gain full control of the affected audio device, including the ability to play audio at high volumes or eavesdrop on conversations through the device's microphone. The vulnerability affected products from multiple major manufacturers, underscoring that unmanaged Bluetooth peripherals can pose a significant risk in environments without continuous visibility into active wireless devices.

4.2 Wi-Fi Chipset and Driver Vulnerabilities

Wi-Fi vulnerabilities disclosed in 2025 affected WLAN drivers and chipsets embedded in access points, routers, laptops, and industrial systems. Reported risks included remote code execution through malformed Wi-Fi frames and privilege escalation within WLAN drivers, often requiring only wireless proximity.

In one example, researchers disclosed a set of high-severity vulnerabilities in MediaTek wireless LAN drivers widely embedded in consumer and enterprise Wi-Fi devices. The flaws originated from out-of-bounds memory handling in the WLAN driver code and could enable local privilege escalation and, in some configurations, remote code execution. Because the vulnerabilities exist at the driver level and require no user interaction once a device is within wireless range, researchers emphasized their broad applicability and potential impact. The disclosures highlighted the systemic risk posed by widely deployed Wi-Fi components that are difficult to inventory, monitor, and remediate across large environments.

4.3 Zigbee Protocol and Mesh Network Weaknesses

Zigbee-related CVEs highlighted weaknesses in authentication, key management, and mesh trust relationships. These vulnerabilities are significant because Zigbee devices often supportoperational or safety functions, operate without continuous monitoring, and lack standardized patch mechanisms.

A representative example is CVE-2025-1221, a Denial-of-Service vulnerability affecting Zigbee Radio Co-Processors that use the Silicon Labs EmberZNet Zigbee stack. Under heavy Zigbee traffic, the affected co-processor may fail to forward messages to the host controller, rendering the device unresponsive until it is hard-reset. This behavior arises from improper handling of internal resources. It can disrupt the normal operation of Zigbee-based mesh networks, which are often used in operational and building automation systems and have limited monitoring and patching capabilities.

4.4 Cellular Vulnerabilities Affecting LTE and 5G

LTE and 5G vulnerabilities disclosed in 2025 affected modem firmware and signaling logic across a range of devices, from mobile endpoints to embedded industrial systems. Public analysis emphasized signaling abuse, denial-of-service conditions, and exploitation paths independent of enterprise IP networks.

One such example is CVE-2025-20753, a remote Denial-of-Service vulnerability affecting modem firmware in numerous MediaTek 5G NR15 and NR16 platforms, as well as several Dimensity series and IoT modem chipsets. The vulnerability arises from an uncaught exception in the modem firmware that can be triggered when a User Equipment (UE) device connects to a rogue or malicious base station controlled by an attacker. Successful exploitation can cause the modem to crash and disrupt device connectivity without requiring any user interaction or additional execution privileges.

Collectively, these cases demonstrate a consistent pattern. Wireless vulnerabilities increasingly affect shared technical foundations rather than isolated products, amplifying exposure and complicating remediation.

5. Looking Forward in 2026

5.1 Vulnerability Trends

Wireless vulnerability growth entering 2026 reflects both an increase in disclosed CVEs and a deeper structural shift in how wireless risk accumulates across enterprise and operational environments. Unlike traditional IT vulnerabilities, wireless CVEs frequently affect protocols, chipsets, and embedded device classes that persist for years and operate outside centralized patching and management frameworks. High-profile disclosures in 2025 demonstrate that wireless weaknesses increasingly originate at foundational layers of connectivity rather than in isolated applications.

Looking forward, the trend suggests that wireless vulnerability exposure will continue to expand across Wi-Fi, Bluetooth, Zigbee, LTE, and 5G environments, particularly as organizations adopt more complex wireless integrations in building systems, industrial control, logistics, and medical infrastructure. The cumulative nature of wireless CVEs means that each year's disclosures compound an already large base of unresolved or partially mitigated weaknesses, especially in long-lived or unpatchable devices. As a result, vulnerability trends in 2026 will likely emphasize persistent protocol-level risk, delayed remediation cycles, and the growing importance of continuous wireless visibility as a foundational requirement for enterprise wireless risk management.

5.2 More Wireless Vulnerabilities

The number of wireless vulnerabilities will continue to rise through 2026 as wireless technologies expand into a broader range of enterprise and critical infrastructure use cases. Organizations increasingly rely on wireless connectivity not only for workforce mobility, but also for operational systems such as building automation, industrial sensors, access control, logistics tracking, and embedded medical and manufacturing devices. Each additional deployment introduces new protocol dependencies, implementation complexity, and exposure pathways that extend beyond traditional network perimeters.

Wireless vulnerability growth will likely remain driven by three reinforcing factors. First, protocol ecosystems such as Wi-Fi, Bluetooth, Zigbee, LTE, and 5G continue to evolve, introducing new features and specifications that increase the likelihood of implementation flaws. Second, widely shared chipsets and software stacks create systemic risk, where a single vulnerability can propagate across multiple vendors and device classes. Third, patching constraints in embedded and operational environments mean that many wireless weaknesses persist long after disclosure, compounding exposure year over year.

As wireless vulnerabilities become more frequent and foundational, enterprises will face increasing difficulty managing risk solely through patch-centric approaches. The expected increase in wireless CVEs in 2026 underscores the need for security models that prioritize continuous awareness of wireless activity, identification of unmanaged devices, and compensating controls in environments where remediation remains limited or slow.

5.3 AI-Enabled Wireless Attacks

5.3.1 AI Automation for Target Discovery and Attack Chaining

Bastille expects attackers to increasingly leverage AI and machine learning to accelerate the discovery of wireless targets and reduce the effort required to execute scalable attacks. They can train machine learning models on RF telemetry, device fingerprints, and publicly available vulnerability data to identify patterns associated with specific wireless technologies, device classes, or protocol behaviors. This capability enables adversaries to prioritize environments with dense Bluetooth peripheral usage, exposed Wi-Fi infrastructure, or unmanaged Zigbee and cellular-connected systems that fall outside traditional security visibility.

In parallel, attackers are likely to deploy automation and AI-assisted decision-making to orchestrate wireless attacks with reduced manual intervention. Automated tooling can scan for nearby wireless activity, attempt opportunistic pairing or protocol interaction, and adapt based on device responses. Generative AI tools can augment adversaries by suggesting exploit code templates or helping operationalize complex protocol knowledge. As wireless environments grow more dynamic and heterogeneous, these AI-augmented reconnaissance and automation techniques could increase the likelihood of opportunistic wireless exploitation, underscoring the need for continuous, evidence-based visibility into ongoing wireless activity.

5.3.2 Nation-State Actors

Nation-state actors are likely to play an increasing role in the evolution of wireless attacks as strategic competition extends into the RF domain. Advanced state-sponsored groups have the resources to integrate AI-driven analytics with custom wireless tooling to conduct persistent reconnaissance, target selection, and exploitation against high-value environments, including government facilities, defense contractors, critical infrastructure, and research institutions. Wireless technologies offer attractive access paths for these actors because they often bypass traditional network defenses, enable proximity-based operations, and intersect with operational systems that are difficult to patch or replace. As AI capabilities mature, nation-state actors may further automate wireless reconnaissance and attack workflows to scale operations, reduce operational risk, and rapidly adapt to newly disclosed vulnerabilities, reinforcing the strategicimportance of continuous wireless visibility for organizations operating in sensitive or regulated sectors.

5.3.3 AI-Enabled Wireless Attacks in the Context of MITRE ATT&CK

From a MITRE ATT&CK perspective, AI-assisted wireless attacks primarily enhance adversary effectiveness across the Reconnaissance, Resource Development, Initial Access, and Discovery tactics. During Reconnaissance (TA0043), attackers may use automation and machine learning to collect and analyze wireless signals, device advertisements, and protocol metadata to identify target environments with dense wireless activity or the presence of specific technologies. This approach aligns with techniques such as Network Service Discovery (T1046) and Active Scanning (T1595), adapted to wireless rather than IP-based environments.

AI can also support Resource Development (TA0042) by lowering the effort required to operationalize wireless attack tooling. Generative models may assist attackers in understanding protocol behavior, generating proof-of-concept exploit code, or adapting publicly disclosed vulnerabilities into usable attack workflows. While AI does not replace technical expertise, it can accelerate preparation and reduce the time between vulnerability disclosure and practical exploitation.

Once in proximity to a target environment, automation and AI-enabled decision logic can streamline Initial Access (TA0001) attempts against wireless technologies. This approach includes opportunistic Bluetooth pairing abuse, Wi-Fi protocol interaction, or signaling manipulation, activities that, when translated to wireless interfaces, are conceptually aligned with techniques such as Exploit Public-Facing Application (T1190). During Discovery (TA0007), automated wireless reconnaissance can help attackers identify active devices, protocols, and configurations without relying on traditional network access, reinforcing the value of continuous wireless visibility for defenders.

Overall, AI does not introduce new ATT&CK tactics, but it can significantly increase the speed, scale, and adaptability with which existing tactics apply to wireless environments. This convergence reinforces the importance of controls that provide real-time awareness of wireless activity, as traditional ATT&CK-mapped defenses often assume IP-based visibility that does not extend to RF-layer attack paths.

6. The Wireless Visibility Gap

Despite the acceleration of wireless CVE disclosures, most organizations lack continuous insight into wireless activity. Traditional vulnerability management approaches emphasize asset inventories, authenticated scanning, and patch metrics. These controls do not reliably capture:

- Known but unmanaged devices, such as personal Bluetooth peripherals
- Unknown and unmanaged devices, including embedded Zigbee systems
- Transient or third-party wireless equipment
- Cellular-connected systems operating outside enterprise networks

Without real-time visibility into active wireless protocols and devices, organizations struggle to assess relevance and prioritize response following CVE disclosure.

7. Bastille Key Findings and Recommendations

7.1 Key Findings

- Wireless CVEs are expanding at a sustained 25% annual growth rate.
- Compounding accumulation increases persistent exposure.
- Shared protocol stacks amplify systemic risk.
- Wireless exploitation often bypasses traditional IP-centric controls.
- Visibility limitations represent the primary structural weakness in enterprise wireless risk management.

7.2 Bastille Recommendations

Near-term: Organizations should establish continuous, passive wireless monitoring to gain immediate visibility into unmanaged and non-IP wireless devices.

Medium-term: Organizations should integrate wireless visibility into existing vulnerability management, incident response, and risk governance processes so wireless context informs triage, investigation, and prioritization alongside traditional IT telemetry.

Strategic: Enterprises should treat wireless visibility as foundational security infrastructure and extend coverage beyond Wi-Fi and Bluetooth to include Zigbee and cellular technologies such as LTE and 5G.

Bastille aligns with these recommendations through 100% passive monitoring and RF spectrum analysis, supporting wireless awareness without operational disruption.

8. Bastille's Role in Wireless CVE Risk Management

Bastille provides continuous, 100% passive monitoring of the wireless environment across Wi-Fi, Bluetooth, Zigbee, LTE, and 5G. By directly observing wireless activity in the RF spectrum, Bastille delivers visibility independent of device configuration, network enrollment, or asset ownership.

8.1 Why RF-Spectrum-Level Visibility Matters

RF-spectrum-level observation does not require device cooperation or proper configuration. Organizations can observe wireless activity even when devices are unmanaged, misconfigured, transient, or deliberately hidden, improving confidence in situational awareness. RF visibility complements, rather than replaces, existing security controls.

8.2 Operational Outcomes Enabled by Bastille

Continuous wireless visibility supports:

- Improved awareness following disclosure of new wireless vulnerabilities
- Reduced uncertainty during the investigation of wireless-related security events
- More informed compensating control decisions when remediation options are limited
- Improved coordination across security, facilities, and operational teams

8.3 Complementing Existing Security Controls

Bastille does not replace vulnerability scanners, endpoint tools, or network monitoring platforms. Instead, it provides visibility where those controls lack coverage and supplies context that informs existing security and risk workflows.

8.4 Use-Case Context for Wireless CVE Management

Bastille is particularly relevant in scenarios such as:

- Awareness and understanding of wireless technologies present in a facility following the disclosure of new wireless vulnerabilities
- Investigation support for anomalous or unknown wireless activity observed during security incidents
- Ongoing visibility in environments with long-lived or unpatchable wireless devices

8.5 Supporting Risk Governance and Assurance

By providing defensible evidence of wireless activity, Bastille supports audit readiness, compliance reporting, and executive decision-making by reducing reliance on assumptions when assessing wireless risk.

9. Conclusion

Wireless CVE growth in 2024 and 2025 reflects a lasting transformation in the enterprise threat landscape. Vulnerabilities affecting Wi-Fi, Bluetooth, Zigbee, LTE, and 5G represent persistent exposure driven by protocol reuse, device longevity, and limited visibility.

As wireless technologies continue to expand into operational and critical environments, visibility gaps will increasingly shape risk outcomes. Continuous wireless monitoring provides a practical foundation for addressing this challenge. Bastille supports this approach by providing real-time insight into the wireless environment and enabling informed, defensible wireless risk-management decisions.

About the Author

Dr. Brett Walkenhorst, Chief Technology Officer, Bastille

Brett is the CTO of Bastille, where he leads R&D efforts to enhance product performance and add new capabilities. He has over 20 years of experience as a technology leader in RF systems and signal processing. Prior to Bastille, he led and executed R&D efforts at Lucent Bell Labs, GTRI, NSI-MI Technologies, Silvus Technologies, and Raytheon Technologies. His experience includes RF system design, communications systems, antenna design/testing, radar, software-defined radios, geolocation, and related topics. He has authored over 70 publications including papers, articles, and reports, has taught numerous graduate, undergraduate, and professional short courses, and has served as an expert witness on multiple occasions. He is a senior member of IEEE and has served as the Chair of the Atlanta Chapter of the IEEE Communications Society.

About Bastille

Bastille specializes in providing security solutions for wireless environments. Bastille uses a network of Software-Defined Radios (SDRs) to continuously monitor a facility's entire wireless environment, including cellular, Bluetooth Classic, Bluetooth Low Energy (BLE), Wi-Fi, Zigbee, and other protocols. Our sensors detect, analyze, and localize transmissions in real time, providing a comprehensive view of wireless activity.

Bastille's system goes beyond just identifying signals; it analyzes data to uncover real-time and long-term threats. By capturing the entire wireless spectrum, Bastille offers unparalleled visibility into potential security risks, empowering organizations to proactively safeguard their wireless infrastructure. Learn more at bastille.net.

Appendix 1: High Profile Wireless Vulnerabilities in 2025

CVE ID	Protocol/ Domain	Affected Component	Vulnerability Type	Impact Summary	Notable Risk Characteristics
CVE-2025-35971	Wi-Fi	Intel PROSet / Wireless Wi-Fi drivers	Out-of-bounds write	Denial of Service	Triggerable without authentication; affects widely deployed Wi-Fi drivers
CVE-2025-20631/ 20632/20633	Wi-Fi	MediaTek WLAN drivers	Memory corruption (OOB write)	Privilege escalation; potential RCE	Driver-level flaw; impacts millions of embedded and infrastructure devices
CVE-2025-36911 (WhisperPair)	Bluetooth	Consumer Bluetooth audio devices	Forced pairing / authentication bypass	Device takeover; eavesdropping	No user interaction; pairing within ~14 meters; affects major brands
CVE-2025-44557	BLE	Cypress PSoC4 BLE stack	State machine flaw	Authentication bypass	Affects embedded BLE devices; protocol-level weakness
CVE-2025-59289	Bluetooth (Windows)	Windows Bluetooth Service	Use-after-free	Local privilege escalation	Escalates to SYSTEM; affects enterprise endpoints
CVE-2025-1221	Zigbee	Silicon Labs EmberZNet RCP	Resource handling flaw	Denial of Service	Impacts mesh networks; can disrupt building automation and IoT systems
CVE-2025-20753	Cellular (5G/LTE)	MediaTek modem firmware	Uncaught exception	Remote Denial of Service	Triggered via rogue base station; no user interaction required
CVE-2025-6599	Cellular (4G/5G CPE)	Zyxel LTE/5G routers	Resource exhaustion	Denial of Service	Affects the edge and CPE infrastructure
CVE-2025-27840	IoT (Wi-Fi / Bluetooth SoC)	ESP32 microcontroller	Undocumented command abuse	Memory manipulation / compromise	Impacts millions of IoT devices using a shared chipset
CVE-2025-65824	IoT (BLE OTA)	BLE-enabled IoT device firmware	Missing integrity validation	Remote Code Execution	Unauthenticated OTA firmware update abuse

Appendix 2: Wireless Threat Inventory

The following is an inventory of Threats and Assessment Tests Bastille performs as part of a Wireless Threat Assessment. The inventory supplements Bastille's latest research on wireless threats and provides a sample of threat categories that the Bastille system can actively identify through continuous wireless monitoring.

Each item includes a description of the Threat or Assessment Test, the associated MITRE ATT&CK Tactics, and the testing methodology used to determine the threat's presence or the test result. The Threat Level depends on the use case. However, the levels listed below assume a moderate security policy that highlights malicious activity while allowing for a liberal amount of wireless activity and mechanisms to investigate potential misconfigurations.

A2.1 - Threat Level: Critical

Item	Threat Description
[BN-S1-WIFI-ETA]	Evil Twin Access Point
[BN-S1-RF-MAL]	Malicious Device
[BN-S1-RF-MAC]	MAC Spoofing

A2.1.1 - [BN-S1-WIFI-ETA] Evil Twin Access Point

Description	An unauthorized AP that spoofs a legitimate SSID and characteristics to misdirect clients, enabling credential harvesting or MiTM attacks.
MITRE ATT&CK Tactics	Defense Evasion, Credential Access, Collection, Exfiltration
Test Methodology	Passive analysis of BSSID signatures and signal metadata to identify unauthorized hardware broadcasting legitimate network identifiers.

A2.1.2 - [BN-S1-RF-MAL] Malicious Device

Description	Identification of known attack platforms (e.g., Flipper Zero, Wi-Fi Pineapple) used to automate wireless exploitation or keystroke injection.
MITRE ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access, Execution, Defense Evasion, Credential Access, Lateral Movement, Collection, Command & Control, Exfiltration, Impact
Test Methodology	Monitoring for protocol-specific advertising signatures and behavioral patterns unique to known penetration testing and exploitation hardware.

A2.1.3 - [BN-S1-RF-MAC] MAC Spoofing

Description	The unauthorized modification of a wireless interface address to impersonate a trusted device and bypass access controls.
MITRE ATT&CK Tactics	Initial Access, Execution, Privilege Escalation, Defense Evasion, Credential Access, Lateral Movement, Collection, Command & Control, Exfiltration
Test Methodology	Analysis of PHY-layer fingerprints and OUI metadata to detect inconsistencies between a device's reported identity and its RF behavior.

A2.2 - Threat Level: Investigate

Item	Threat Description
[BN-S2-RF-LIVE]	Audio/Video Livestreaming
[BN-S2-WIFI-MULT]	Clients Connecting to Multiple Wi-Fi Networks
[BN-S2-WIFI-ROGN]	Rogue Access Points
[BN-S2-RF-UNAUTH]	Unauthorized Devices
[BN-S2-BLE-ECRP]	Excessive Connection Request Packets
[BN-S2-BT-EIP]	Excessive Inquiry Packets
[BN-S2-BLE-ESRP]	Excessive Scan Request Packets
[BN-S2-WIFI-EPP]	Excessive Wi-Fi Probe Packets
[BN-S2-BT-IBN]	Infrastructure Bluetooth Networks
[BN-S2-ZIG-BEA]	Zigbee Beacon Attack
[BN-S2-ZIG-REJ]	Zigbee Rejoin Attack
[BN-S2-ZIG-COUN]	Zigbee Security Counter Attack
[BN-S2-ZIG-ENER]	Zigbee Energy Depletion Attack
[BN-S2-ZIG-PANID]	Zigbee PAN ID Collision Attack
[BN-S2-BLE-SOUR]	Sour Apple BLE Attack
[BN-S2-BLE-PACS]	PACSMAN Brute-Force Connection Attack
[BN-S2-RF-RFJ]	RF Jammer
[BN-S2-CELL-UCA]	Unusual Cellular Activity
[BN-S2-WIFI-WDJ]	Wi-Fi Deauthentication/Disassociation Attack
[BN-S2-WIFI-RTS]	Wi-Fi RTS/CTS Abuse
[BN-S2-WIFI-FLOOD]	Wi-Fi Packet Flooding Attack
[BN-S2-WIFI-WEP]	Use of Deprecated Wireless Encryption

A2.2.1 - [BN-S2-RF-LIVE] Audio/Video Livestreaming

Description	The transmission of any audio or video capture wirelessly can be concerning when detected in very sensitive environments. When detected, particularly in geofenced areas containing highly sensitive material, documents, or discussions, this threat may warrant elevation to critical. In most cases, security teams should investigate the transmission of such data as time allows.
MITRE ATT&CK Tactics	Reconnaissance
Test Methodology	Various packet types across several protocols offer clues about the type of data the emitter is transmitting. When Bastille detects that an emitter is transmitting audio or video data, the system tags those emissions so operators can investigate further.

A2.2.2 - [BN-S2-WIFI-MULT] Clients Connecting to Multiple Wi-Fi Networks

Description	When both open, insecure Wi-Fi networks and secure, encrypted Wi-Fi networks are present, observing Wi-Fi clients using both can raise concerns. If clear-text data were transmitted inadvertently over an insecure network, it could be intercepted and viewed.
MITRE ATT&CK Tactics	Defense Evasion, Lateral Movement
Test Methodology	Analyze all Wi-Fi clients and determine their SSID connection history. If clients are using both secure and insecure networks, annotate these devices for further investigation.

A2.2.3 - [BN-S2-WIFI-ROGN] Rogue Access Point Detected

Description	Rogue Access Points are those that are neither supported nor authorized but are accessible within the monitored space. This category includes unauthorized APs, hotspots, and any unauthorized device based on its BSSID and ESSID. These access points may be within the monitored space or near it, providing Wi-Fi connectivity to devices.
MITRE ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access, Persistence, Credential Access, Discovery, Collection, Command and Control, Impact
Test Methodology	The Bastille system scans the Wi-Fi airspace for all advertising or in-use SSIDs and compares them against the customer-provided list of authorized Wi-Fi networks. The Bastille system provides an inventory of discovered SSIDs, indicating whether any Wi-Fi clients used any of them during the assessment period.

A2.2.4 - [BN-S2-RF-UNAUTH] Unauthorized Devices

Description	Security teams should investigate unauthorized devices identified by operator-issued lists of authorized devices and RF baselines. Highly sensitive environments may require elevating this risk profile. Geofences may also be applied to refine the risk level. This geofence can include access points, endpoints, controllers, peripherals, etc. By itself, the presence of an unauthorized device may not be deemed a high risk, but when combined with other events, this designation provides useful context.
MITRE ATT&CK Tactics	Reconnaissance, Initial Access, Discovery
Test Methodology	Analyze new devices relative to the RF baseline and user-provided data.

A2.2.5 - [BN-S2-BLE-ECRP] Excessive Connection Request Packets

Description	Connection Requests occur in the normal Bluetooth Low Energy (BLE) connection lifecycle. Seeing a few of these a day is not abnormal. However, seeing many connection requests, especially from one device to many others within a short period, is analogous to a burglar trying door handles to find one that is unlocked and is a clear threat indicator.
MITRE ATT&CK Tactics	Reconnaissance, Discovery
Test Methodology	Analysis of the collected BLE metadata to determine the overall volume and sources of BLE Connection Request transmissions. Review the collected data to determine if there are significant volumes and the sources of those high volumes of Connection Request requests.

A2.2.6 - [BN-S2-BT-EIP] Excessive Inquiry Packets

Description	The transmission of Bluetooth Inquiry Packets is a normal part of network behavior, so they may always be present. However, a high volume of Inquiry packets relative to other network devices may indicate that a device is attempting to map or discover Bluetooth network assets.
MITRE ATT&CK Tactics	Reconnaissance, Discovery
Test Methodology	Aggregate all Bluetooth Inquiry packets and sort them by top transmitters. Compare these top transmitters with the remainder of the population to establish a baseline for Inquiry packet levels in the environment. Identify devices exhibiting above-expected Inquiry packet generation rates.

A2.2.7 - [BN-S2-BLE-ESRP] Excessive Scan Request Packets

Description	An excessive number of Scan request packets indicates that a Bluetooth Low Energy (BLE) device may be wardriving or mapping the BLE network of an environment. While this behavior can originate from a poorly configured, innocuous device, it is also the pattern of packets one would observe from an attacker attempting to enumerate all devices to identify vulnerabilities.
MITRE ATT&CK Tactics	Reconnaissance, Discovery
Test Methodology	Analysis of the collected BLE metadata to determine the overall volume and sources of BLE Scan request transmissions. Review the collected data to determine if there are significant volumes and the sources of those high volumes of Scan requests.

A2.2.8 - [BN-S2-WIFI-EPP] Excessive Wi-Fi Probe Packets

Description	The transmission of Wi-Fi Probe Packets is normal network behavior, so they may always be present. However, a high volume of Probe packets relative to other network devices may indicate that a device is attempting to map or discover Wi-Fi network assets.
MITRE ATT&CK Tactics	Reconnaissance, Discovery
Test Methodology	Aggregate all Wi-Fi Probe packets and sort them by top transmitters. Compare these top transmitters with the remainder of the population to establish a baseline for Probe packet levels in the environment. Identify devices exhibiting above-expected Probe packet generation rates.

A2.2.9 - [BN-S2-BT-IBN] Infrastructure Bluetooth Networks

Description	Infrastructure systems manifest through the RF spectrum as persistent transmitters. Security teams should identify and explicitly authorize persistent Bluetooth transmitters and connections to ensure that Bluetooth does not expose data leaks or control surfaces.
MITRE ATT&CK Tactics	Initial Access, Execution, Defense Evasion, Lateral Movement, Command & Control, Impact
Test Methodology	Collect the inventory of all Bluetooth transmitting endpoints, their metadata, and locations. Verify that each discovered Bluetooth device is authorized to be present in the monitored area.

A2.2.10 - [BN-S2-ZIG-BEA] Zigbee Beacon Attack

Description	Attackers may use Zigbee beacons to conduct reconnaissance, shut down networks, orphan endpoints, and eventually gain unauthorized access to a network.
MITRE ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access, Defense Evasion, Impact
Test Methodology	Analyze the beacons originating from a single device, based on device ID, location, etc., over time, to determine whether the activity is malicious.

A2.2.11 - [BN-S2-ZIG-REJ] Zigbee Rejoin Attack

Description	Detection of "Unsecured Rejoin" requests that allow an attacker to join a Zigbee mesh without a valid network key.
MITRE ATT&CK Tactics	Initial Access, Execution, Privilege Escalation, Defense Evasion, Credential Access, Lateral Movement, Collection, Command & Control, Exfiltration
Test Methodology	Passive analysis of Zigbee NWK layer metadata to identify Rejoin Request frames where security headers or keys are absent or improperly formatted.

A2.2.12 - [BN-S2-ZIG-COUN] Zigbee Counter Attack

Description	Detection of anomalies in frame counters (802.15.4, NWK layer, and Security Header) that attackers use to facilitate denial of service and replay attacks.
MITRE ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access, Defense Evasion, Impact
Test Methodology	Continuous monitoring of Zigbee frame headers to identify non-sequential jumps, resets, or repeated counter values across the MAC and NWK layers.

A2.2.13 - [BN-S2-ZIG-ENER] Zigbee Energy Depletion Attack

Description	A targeted attack (e.g., Zigator) sends max-sized frames with default sequence numbers to drain the batteries of IoT/OT endpoints.
MITRE ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access, Defense Evasion, Impact
Test Methodology	Analysis of Zigbee frame sizes and transmission intervals to identify patterns of "keep-awake" traffic that deviate from standard device power-save behavior.

A2.2.14 - [BN-S2-ZIG-PANID] Zigbee PAN ID Collision Attack

Description	Detection of intentional conflicts with a Zigbee Personal Area Network (PAN) ID. This attack aims to cause network instability or force devices to disconnect by spoofing or duplicating an existing PAN ID.
MITRE ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access, Defense Evasion, Impact
Test Methodology	Detection of conflicting PAN ID advertisements or specific collision notification frames within the monitored RF environment.

A2.2.15 - [BN-S2-BLE-SOUR] Sour Apple BLE Attack

Description	Flooding devices with proximity notification spam, which can cause iOS devices to lock up and force a reboot (DoS).
MITRE ATT&CK Tactics	Impact
Test Methodology	Monitoring for rapid bursts of BLE advertisement payloads specifically formatted to trigger proximity pairing or notification actions on mobile operating systems.

A2.2.16 - [BN-S2-BLE-PACS] PACSMAN Brute-Force Connection Attack

Description	Documented at DEFCON 2021, the PACSMAN attack is a denial-of-service attack on BLE devices. Repeated connection-request packets enable the attack.
MITRE ATT&CK Tactics	Impact
Test Methodology	Analysis of the collected BLE metadata to determine the overall volume and sources of BLE Connection Request transmissions. Review the collected data to determine if there are significant volumes and the sources of those high volumes of Connection Request. Note the high-volume transmitters of Connection Request packets in the assessment.

A2.2.17 - [BN-S2-RF-RFJ] RF Jammer

Description	Attackers can use an RF jammer to deny service for multiple protocols within a given frequency band. This attack can take the form of a cellular jammer, a GPS jammer, a Wi-Fi jammer, or a more generic jammer. The presence of unusually high levels of energy in certain bands, particularly over short time durations, can indicate the presence of such a jammer.
MITRE ATT&CK Tactics	Impact
Test Methodology	Analyze the collected spectrum survey data from the Bastille system to detect any increase in RF traffic during the assessment period. Record frequencies observed, timeline, and location in the assessment report.

A2.2.18 - [BN-S2-CELL-UCA] Unusual Cellular Activity

Description	Unusually high levels of cellular activity can indicate an unauthorized presence in the facility and/or unauthorized data transfer that bypasses network security. The presence of cellular transmissions within or near the monitored space may not violate the wireless security policy. However, analysts should use the collected data to determine whether appropriate use is occurring.
MITRE ATT&CK Tactics	Defense Evasion, Collection, Exfiltration
Test Methodology	Collect Cellular metadata from the collection period and analyze cellular transmissions for all detected devices. Identify the cellular top-talkers and record their metadata, including location history, in the assessment report.

A2.2.19 - [BN-S2-WIFI-WDJ] Wi-Fi Deauthentication/Disassociation Attack

Description	Several popular attacks for obtaining Wi-Fi network keys require observing multiple client-to-access point connections. To expedite the process, many attacks automate the generation of Wi-Fi traffic that causes clients to disconnect from APs. The attacker can then gather the clients' reconnection attempts for later analysis. Additionally, flooding the network with deauthentication and/or disassociation traffic can cause Wi-Fi clients to disconnect; depending on client configuration, they may reconnect to a different network with weaker security controls or to a man-in-the-middle Wi-Fi access point.
MITRE ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access, Defense Evasion, Impact
Test Methodology	The Bastille system analyzes Wi-Fi metadata it captures to detect significant volumes of Deauthentication and Disassociation traffic. If found, the Bastille system notes the sources and their location in the assessment.

A2.2.20 - [BN-S2-WIFI-RTS] Wi-Fi RTS/CTS Abuse

Description	Detection of abnormal Wi-Fi "Request to Send" (RTS) or "Clear to Send" (CTS) traffic. This activity includes frames with excessively high "Duration" values designed to silence medium or high-volume flooding.
MITRE ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access, Defense Evasion, Impact
Test Methodology	Analysis of captured RF metadata to identify non-standard duration field values and high-frequency RTS/CTS frame bursts that lack corresponding data transmission.

A2.2.21 - [BN-S2-WIFI-FLOOD] Wi-Fi Packet Flooding Attack

Description	Attackers can flood management frames (Beacons, Probes, Auth) not covered by other categories to overwhelm AP/client resources.
MITRE ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access, Defense Evasion, Impact
Test Methodology	Monitoring RF metadata for abnormal volumes of specific Management Frame types (Type 0) that exceed baseline behavioral thresholds for the environment.

A2.2.22 - [BN-S2-WIFI-WEP] Use of Deprecated Wireless Encryption

Description	Introduced in 1997, Wired Equivalent Privacy (WEP) was once the standard Wi-Fi encryption, but it's no longer secure due to advances in computing power and is now readily compromised. WEP uses a single key to secure an entire network and does not provide per-user or per-session encryption; once WEP keys are compromised, the entire network becomes accessible to a malicious user. Today, it's a trivial matter for even a consumer-grade computer to run the calculations needed to decrypt a WEP key. The WEP security protocol was retired in 2004, and any system still using it should be updated or replaced
MITRE ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access
Test Methodology	The Bastille system analyzes the Wi-Fi metadata it captures to assess the use of the WEP encryption protocol. If found, the Bastille system notes the sources and locations in the assessment.

A2.3 - Threat Level: Awareness

Item	Threat Description
[BN-S3-RF-TRACK]	Wireless Tracker Devices
[BN-S3-RF-DEV]	Wireless A/V or VR/AR Devices
[BN-S3-RF-AV]	Audio/Video Capability
[BN-S3-WIFI-OPEN]	Open, Unencrypted Networks Present
[BN-S3-WIFI-ENC]	Weak encryption
[BN-S3-WIFI-SSID]	Invalid SSID length
[BN-S3-WIFI-DIRECT]	Wi-Fi Direct
[BN-S3-BLE-INVA]	Invalid BLE Random Address
[BN-S3-RF-FCC]	FCC Covered Products Detected

A2.3.1 - [BN-S3-RF-TRACK] Wireless Tracker Devices

Description	Presence of mobile tracking tags (e.g., AirTag, Tile) that utilize crowd-sourced networks for persistent location reporting.
MITRE ATT&CK Tactics	Reconnaissance
Test Methodology	Passive analysis of RF metadata to identify periodic, manufacturer-specific advertising intervals and signal strengths consistent with a localized tracking device.

A2.3.2 - [BN-S3-RF-DEV] Wireless A/V or VR/AR Devices

Description	The presence of certain devices poses a risk in sensitive environments. The ability to capture audio, video, or both can enable exfiltration of that data for continuous, active surveillance. Examples of such devices include Meta AI glasses, Ray-Ban Stories, Plaud Note, AirPods, etc.
MITRE ATT&CK Tactics	Reconnaissance
Test Methodology	Devices such as smart glasses and AirPods contain specific pieces of metadata that provide clues to signatures the Bastille system can detect over the air. Bastille identifies such devices and tags them for investigation.

A2.3.3 - [BN-S3-RF-AV] Audio/Video Capability

Description	The presence of any audio or video capture capability can be concerning when detected in very sensitive environments. While not identifying specific devices, such as those found in **[BN-S3-RF-DEV]**, this category identifies generic A/V capture capability in wireless emissions.
MITRE ATT&CK Tactics	Reconnaissance
Test Methodology	Packets that provide insight into form factor, capabilities, etc., are assessed and flagged when they indicate the presence of audio or video capture capability.

A2.3.4 - [BN-S3-WIFI-OPEN] Open, Unencrypted Networks Present

Description	Evaluation of Wi-Fi traffic to look for open, unencrypted networks. Organizations typically use unencrypted networks as "Guest" networks, with connectivity limitations intended to prevent access to secure Wi-Fi networks. The presence of open, unencrypted networks is not, in itself, of immediate concern; however, clients configured to connect to both Guest and Secure networks may inadvertently transmit sensitive data over an insecure network. The presence of Open, Unsecured access points enables attackers to more readily conduct the **[BN-S1-WIFI-ETA] Evil Twin Access Point** attack in the environment.
MITRE ATT&CK Tactics	N/A
Test Methodology	Scan all Wi-Fi SSIDs to determine their security posture and configuration.

A2.3.5 - [BN-S3-WIFI-ENC] Weak Encryption

Description	While open networks pose obvious risks, the use of weak encryption schemes increases the risk of network compromise. Identification of weak encryption schemes warrants investigation, though it is typically less urgent than mitigating completely unencrypted networks.
MITRE ATT&CK Tactics	N/A
Test Methodology	Networks advertise their encryption capabilities in various ways across different packet types. The Bastille system analyzes these packets to identify when encryption is less secure than expected.

A2.3.6 - [BN-S3-WIFI-SSID] Invalid SSID Length

Description	An invalid SSID can trigger unwanted behaviors in receiving devices, potentially leading to denial-of-service attacks. At the very least, such an identification indicates a misconfigured device and should be investigated and remediated.
MITRE ATT&CK Tactics	Impact
Test Methodology	The Bastille system inspects and analyzes SSIDs to determine whether they meet the appropriate conditions.

A2.3.7 - [BN-S3-WIFI-DIRECT] Wi-Fi Direct

Description	The presence of a Wi-Fi Direct network typically indicates a configuration intended for ease of use. However, it often reveals to would-be attackers that a dual-homed device is present on the network. Attackers can exploit such configurations to gain access and pivot to penetrate layers of the network that are not otherwise accessible. Bastille recommends that administrators minimize or eliminate the presence of such networks.
MITRE ATT&CK Tactics	Impact
Test Methodology	Wi-Fi Direct networks advertise themselves quite openly. Bastille inspects the beacons of all SSIDs and determines whether any of these networks are present in the facility.

A2.3.8 - [BN-S3-BLE-INVA] Invalid BLE Random Address

Description	BLE addresses have specific constraints depending on their type. A malicious actor may configure addresses in a way that does not conform to the specification. These addresses indicate a poorly configured benign device, and the security team should investigate them.
MITRE ATT&CK Tactics	Impact
Test Methodology	The pattern of viable addresses is straightforward. As the Bastille system detects unique BLE devices, it assesses whether their addresses comply with the specification.

A2.3.9 - [BN-S3-RF-FCC] FCC Covered Products Detected

Description	Presence of hardware from manufacturers identified by the FCC as national security risks (e.g., Secure Networks Act).
MITRE ATT&CK Tactics	Reconnaissance, Resource Development, Initial Access, Persistence, Defense Evasion
Test Methodology	Passive comparison of observed MAC/OUI metadata against the FCC's list of covered entities.

Bastille

About us

Bastille specializes in providing security solutions for wireless environments. Bastille uses a network of Software-Defined Radios (SDRs) to continuously monitor a facility's entire wireless environment, including cellular, Bluetooth Classic, Bluetooth Low Energy (BLE), Wi-Fi, Zigbee, and other protocols. Our sensors detect, analyze, and localize transmissions in real time, providing a comprehensive view of wireless activity.

Bastille's system goes beyond just identifying signals; it analyzes data to uncover real-time and long-term threats. By capturing the entire wireless spectrum, Bastille offers unparalleled visibility into potential security risks, empowering organizations to proactively safeguard their wireless infrastructure.

Learn more

To learn more please visit
www.bastille.net

or follow us on

03/26