

Bluetooth Vulnerabilities

Quick Reference Guide for Security Leaders

The Visibility Challenge

Most organizations can accurately inventory laptops, servers, smartphones, and network infrastructure. Far fewer can identify all Bluetooth devices operating within their facilities.

- Bluetooth technology now supports:
 - Headsets and earbuds
 - Wireless keyboards and mice
 - Smart watches and fitness trackers
 - Mobile devices
 - Medical devices
 - Industrial sensors
 - Smart building technologies
 - Access control systems
 - IoT devices

Many of these devices operate outside traditional asset inventories and security monitoring workflows.

Why Bluetooth Remains a Security Risk

Bluetooth security has improved significantly over the past two decades, but vulnerabilities continue to emerge due to:

Protocol Complexity

Bluetooth relies on thousands of pages of specifications and numerous device profiles, creating opportunities for implementation errors.

Vendor Implementations

Device manufacturers depend on third-party chipsets, firmware, and SDKs that may contain vulnerabilities.

Legacy Devices

Many Bluetooth-enabled devices:

- No longer receive updates
- Receive updates infrequently
- Remain deployed long after vendor support ends

Convenience Features

Technologies such as Fast Pair, Nearby Pairing, and Swift Pair improve usability but can introduce additional attack surface.

Why Traditional Security Tools Miss Bluetooth Activity

Most security tools focus on:

- Network traffic
- Endpoints
- Cloud workloads
- Identity systems

Bluetooth activity often exists outside those monitoring layers.

As a result, many organizations cannot easily answer:

- What Bluetooth devices operate within our facilities?
- Which devices connect to enterprise assets?
- Which devices violate policy?
- Which devices remain active after hours?
- Which devices may expose known vulnerabilities?

Business Risks

A compromised Bluetooth device may provide an attacker with access to systems containing:

- Sensitive business information
- Intellectual property
- Operational technology data
- Healthcare records
- Financial information

Bluetooth represents one component of the broader wireless attack surface that many organizations cannot fully see.

Compliance & Governance Considerations

Bluetooth visibility supports:

- Asset inventory programs
- Continuous monitoring initiatives
- Risk management efforts
- Security policy enforcement
- Regulatory and framework requirements

Organizations often discover gaps between documented assets and actual wireless activity occurring within their environments.

How Bastille Helps

Bastille provides continuous, 100% passive monitoring of the RF spectrum to help organizations:

- Discover Bluetooth-enabled devices
- Identify unauthorized wireless activity
- Detect policy violations
- Investigate suspicious behavior
- Improve wireless asset visibility
- Reduce wireless risk

By providing visibility into Bluetooth devices and other wireless activity, Bastille helps security teams identify threats and address risks before they become security incidents.

Key Takeaway

You cannot secure Bluetooth devices you cannot see.

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

