REPORT

BISHOPFOX

PRODUCT SECURITY REVIEWS

THE BASICS ARE THE BREACH

INTRODUCTION: THE STATE OF PRODUCT SECURITY

Bishop Fox is an expert at delivering hands-on product security reviews for leading organizations across industries including healthcare, consumer IoT, industrial systems, aviation, financial services, and operational technology. These assessments evaluate real products that shape today's markets and directly impact customer safety, operational resilience, and brand trust. From insulin pumps and smart locks to industrial cameras and embedded controllers, these are the technologies that power our modern world.

Unlike large-scale research that relies on automated code analysis, vulnerability scanning, or the correlation of findings across vast codebases, this report is grounded in deep human analysis. Each finding is drawn from adversary-style testing performed and validated by Bishop Fox security experts.

Across our findings, one pattern has remained consistent: attackers rarely need advanced exploits. They succeed because they take advantage of basic, preventable weaknesses that persist across industries; flaws that lead to product recalls, operational disruptions, regulatory exposure, and erosion of customer trust. For companies manufacturing or integrating connected technologies, product security has become indistinguishable from business security.

This report draws on Bishop Fox product security reviews conducted between 2023–2025.

Through these results, we explore:

- The most common product security weaknesses and why they persist
- How findings vary across industries
- The patterns that explain why attackers are still succeeding
- The business implications of these weaknesses, from regulatory risk to brand trust
- How emerging challenges amplify today's flaws
- A clear path forward for raising the baseline of product security

OUR FINDINGS

The data behind this report turn those patterns into measurable evidence. Across two years of hands-on product testing, Bishop Fox engineers identified recurring weaknesses that demonstrate how security breaks down in practice. These results show where vulnerabilities concentrate, how they differ across industries, and why even seemingly low-impact flaws continue to create real exposure when chained together.

Severity Distribution

To understand the current state of product security, it is useful to look at the severity of issues uncovered. The distribution of findings shows where the greatest risks lie and how attackers exploit them in practice. While only a small fraction of issues were deemed catastrophic on their own, the overwhelming presence of medium and low findings creates fertile ground for compromise.

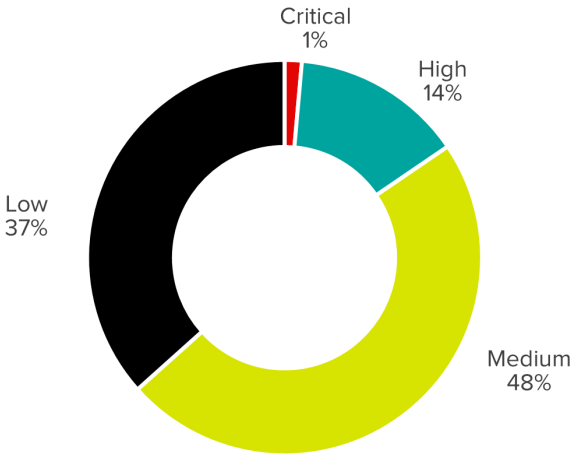


Figure 1: Severity Distribution (%) of PSR engagements

On the surface, the scarcity of critical flaws may appear reassuring. Yet the reality is that medium and low findings made up 75% of all issues. These are the very weaknesses attackers chain together to achieve compromise. A single undocumented API endpoint exposed in production, paired with a missing access control, can be just as damaging as a critical flaw.

In today's connected world, this problem is amplified by accessibility. Many IoT and smart products are readily available for purchase online, giving adversaries unrestricted access to test, probe, and reverse-engineer them at their leisure.

Attackers don't need to find one catastrophic exploit. They win through persistence, time, and creativity until they have an accumulation of small, overlooked weaknesses that together will create a pathway to full compromise.

Note: Bishop Fox severity ratings differ from CVSS because they are grounded in human validation, not automated scoring. Rather than assigning numeric values to theoretical risks, our engineers manually test, exploit, and confirm each issue to determine its actual business impact.

This approach treats severity as a communication tool (reflecting real-world exposure and context), so clients understand not just what could be exploited, but what truly matters.

Most Common Weaknesses Identified

Four categories of flaws consistently appeared across nearly every product: authentication failures, exposed interfaces, weak cryptography, and insecure configurations. These categories tell us not only where manufacturers are falling short, but also where attackers are most likely to strike.

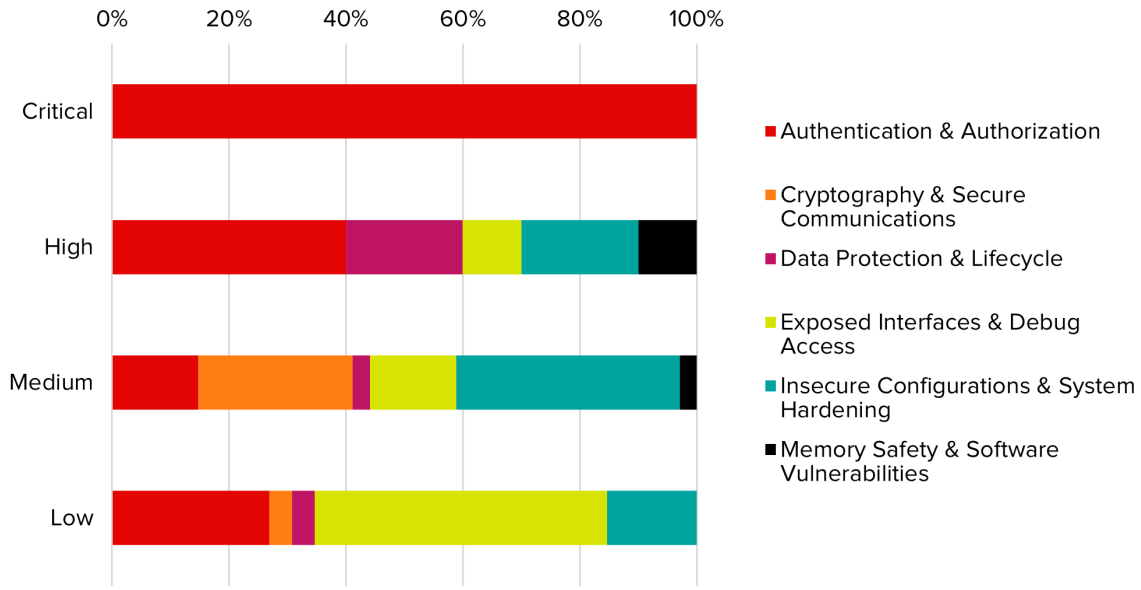


Figure 2: Severity Distribution (%) based on Finding Categories of PSR engagements

AUTHENTICATION AND AUTHORIZATION FAILURES

Weak authentication remains one of the most prevalent issues across industries. Default and shared credentials, reused keys, and missing controls consistently undermine trust in connected products. These flaws are simple for attackers to exploit and open the door to larger compromise.

- Reuse of the same network key across devices
- Use of universal SSIDs and passwords
- Default or shared root accounts
- Missing or weak authentication mechanisms

EXPOSED INTERFACES & DEBUG ACCESS

Products frequently shipped with debug and administrative interfaces still enabled in production. These backdoors provide attackers with direct access to systems, often bypassing authentication entirely.

- Active USB and display ports on industrial devices not intended to be connected to input devices or displays in the field
- UART consoles accessible with default credentials, or no credentials
- Exposed APIs and network services
- SSH enabled by default on devices not intended for remote console access

CRYPTOGRAPHY & SECURE COMMUNICATIONS

Encryption was widely implemented but often flawed, creating a false sense of security. Weak or misapplied cryptography undermined protections that organizations rely on to protect sensitive data and transactions.

- TLS certificate validation disabled or misconfigured
- Predictable or hard-coded encryption keys
- Weak, outdated, or insecurely configured cryptographic algorithms

INSECURE CONFIGURATIONS & SYSTEM HARDENING

Misconfigurations and unsafe defaults were among the most common findings. These weaknesses allow attackers to escalate privileges, re-exploit patched issues, or abuse legacy features.

- Bootloader misconfigurations and insecure defaults
- APIs disclosing sensitive information
- Services running under excessively privileged credentials
- Firmware rollback enabled, allowing users to intentionally downgrade to vulnerable versions and reintroduce known flaws

Cross-Industry Observations

When comparing findings across industries, distinct differences emerge that go beyond severity. Each sector is shaped by unique pressures, whether that be regulation, product lifecycle, or consumer expectations, and those factors determine which weaknesses surface most often.

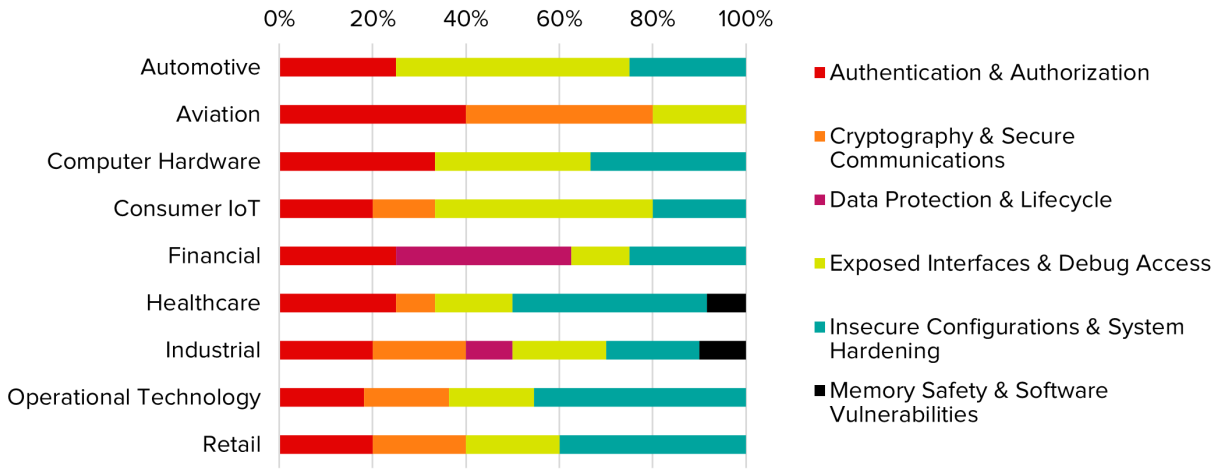


Figure 3: Categorical Distribution (%) based on Industries of PSR engagements

Because representation varied across industries, sector-level insights should be interpreted as directional rather than exhaustive. Where multiple companies were evaluated, we highlight recurring **trends**; where fewer organizations were represented, we note **emerging signals**.

TRENDS

Healthcare: Healthcare devices often had a higher volume of findings, but most were medium or low in severity. Oversight from the FDA and HIPAA drove stronger baseline practices. Cryptography and insecure configurations were most common, underscoring a compliance-driven focus on data protection.

Consumer IoT: Consumer IoT devices repeatedly failed in authentication and exposed interfaces. The absence of strong regulatory pressure and a race-to-market mentality left these products vulnerable to systemic, easy-to-exploit flaws.

EMERGING SIGNALS

Industrial and Operational Technology (OT): Industrial and OT systems carried the highest concentration of critical and high-severity findings. Legacy technologies, long product lifecycles, and insecure defaults were consistent drivers of risk.

Common issues included exposed debug ports, outdated protocols, recurring configuration errors, and default credentials. All of which can enable privilege escalation or operational disruption at scale. While some findings were moderate in isolation, their presence across interconnected environments amplifies systemic exposure.

Financial Services: Financial services assessments highlighted weaknesses in data protection and lifecycle management, such as weak DLP controls and insecure decommissioning. Authentication gaps also persisted, mapping directly to insider misuse and data leakage risks.

Taken together, the industry breakdown highlights that security maturity is not evenly distributed. Regulation, product lifecycle, and market pressure strongly influence outcomes, meaning attackers adapt their tactics by sector. They target default credentials in consumer devices, insecure APIs and outdated protocols in industrial systems, and insider misuse or weak data controls in financial and enterprise environments.

> Findings are aggregated across products and industries to highlight recurring patterns. Industry-level analysis is presented as directional insight, reflecting observed themes where representation allows.

WHAT THE PATTERNS REVEAL

Stepping back from the details of severity levels, categories, and industry differences, several larger themes emerge that explain not just what we found, but why these issues remain so widespread.

Systemic forces outweigh individual choices.

The recurrence of the same categories across industries shows that product security challenges are shaped less by single engineering decisions and more by industry-wide incentives, speed to market, long product lifecycles, or minimal accountability.

Attackers succeed because the fundamentals are weak.

The flaws identified were rarely advanced, but that's precisely the point. Within the defined scope of each engagement, basic issues consistently surfaced first and posed real risk. Many required nothing more than a default password, weak authentication, or a misconfigured service to exploit. This shows that attackers often don't need sophisticated exploits when preventable weaknesses are already exposed in production environments.

Organizations underestimate the "small" issues.

Medium and low findings made up the majority of results. These are often dismissed during risk reviews, yet attackers reliably chain them into real compromises. The gap between perceived and actual risk is one of the most persistent challenges.

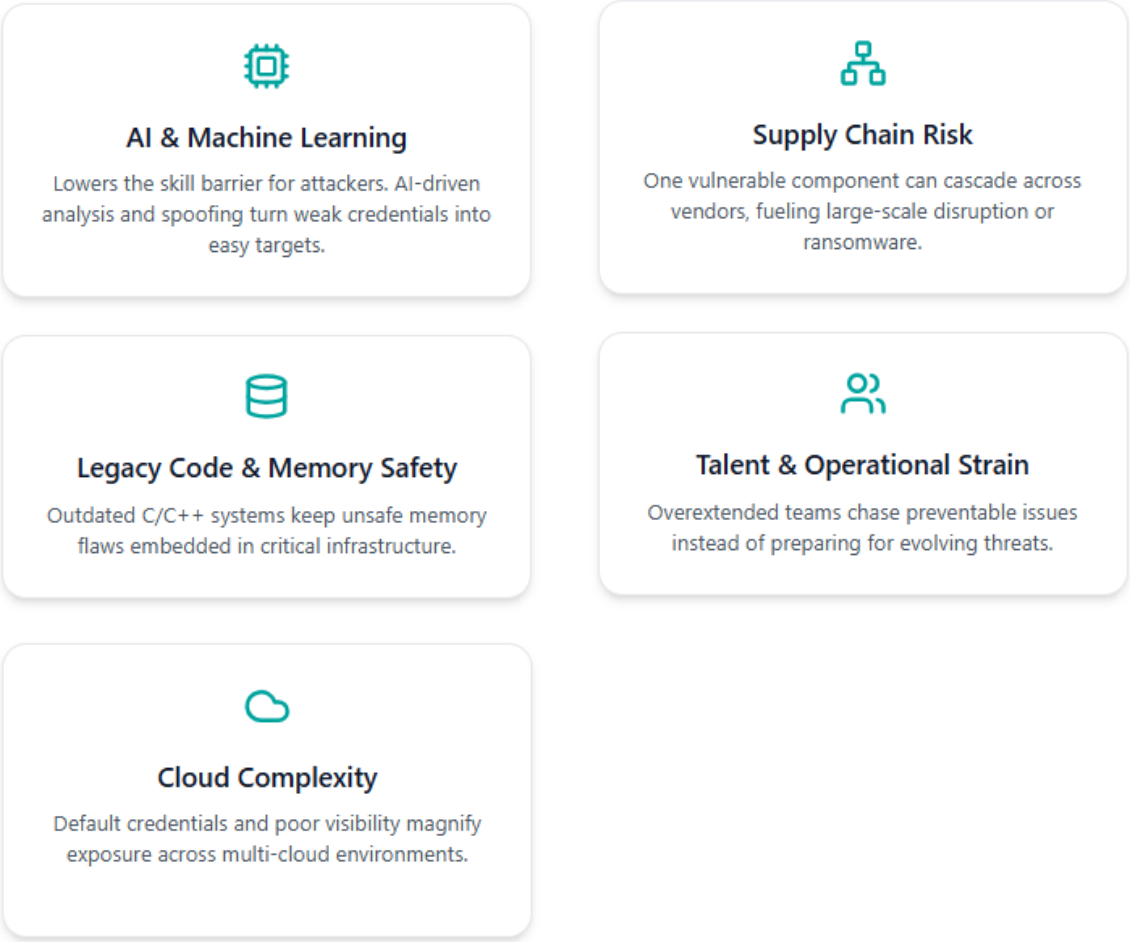
External pressure drives maturity.

Regulation and compliance requirements directly influenced results. Healthcare devices, under FDA and HIPAA oversight, trended toward low-severity issues. In contrast, unregulated sectors like consumer IoT and industrial products repeatedly exposed high-severity weaknesses.

These patterns highlight that product security gaps persist because market and organizational forces make them difficult to prioritize. Until fundamentals are treated as non-negotiable, attackers will continue to find easy success

THE BROADER PRODUCT SECURITY CHALLENGES

The weaknesses identified in our reviews do not exist in isolation. They are amplified by broader challenges that define the current security landscape. These external forces increase both the likelihood of exploitation and the potential scale of impact, turning recurring flaws into systemic risks.



These challenges show that today's recurring product flaws are accelerants, made more urgent by AI, supply chain interdependence, cloud complexity, legacy technology, and talent shortages.

For security leaders, the connection is clear: today's recurring weaknesses map to tomorrow's threats, and both ultimately drive business consequences. The following section explores how these flaws manifest in terms of trust, compliance, and operational resilience.

BUSINESS IMPLICATIONS

The vulnerabilities identified in our reviews are not abstract technical concerns, they have measurable business consequences. Each type of weakness undermines a different dimension of organizational resilience. Understanding these linkages is critical for leaders because the cost of remediation after deployment is not only higher but often accompanied by brand damage and legal liability.

Customer Trust and Market Confidence

Weaknesses that allow products to be manipulated by unauthorized users or that expose personal information erode customer trust at-scale. For example, a smart lock compromised through default credentials is more than a technical flaw; it raises questions about the reliability of the entire brand. In highly competitive markets, trust can be lost quickly and is difficult to rebuild, particularly when customers expect "secure by design" as a baseline.

Regulatory and Legal Exposure

In sectors such as healthcare and finance, insecure defaults or poor cryptographic practices do more than expose data. They frequently constitute violations of government or industry requirements. These findings can lead to regulatory fines, class-action lawsuits, and scrutiny from oversight bodies. In some cases, failure to demonstrate due diligence in product security may even delay product approvals or market access

Operational Disruption and Safety Risk

Industrial and enterprise assessments highlight how seemingly minor flaws can cause large-scale disruption. Weak API protections or exposed administration interfaces in industrial equipment can cascade into downtime across fleets of machines. In aviation or healthcare settings, such weaknesses carry safety implications, as compromised systems can delay operations or endanger lives. The financial impact of disruption often exceeds the direct cost of fixing the flaw.

What makes these implications especially serious is their cumulative nature. A single insecure configuration may be patchable. But across industries, repeated patterns create systemic exposures that affect revenue, compliance, and brand reputation simultaneously.

BISHOP FOX'S PRODUCT SECURITY REVIEW

Are You Prepared to Face the Adversary? Testing Approach

Bishop Fox's Product Security Review (PSR) provides a structured, attacker-focused assessment of connected products. The methodology is designed to identify both common and systemic weaknesses before they can be exploited in the field.

Testing Approach

- Automated testing to uncover a variety of common issues
- Manual penetration testing to replicate real-world adversary tactics across interfaces and protocols
- Code and configuration review to identify misapplied cryptography, insecure defaults, and other design flaws that automated testing misses

Outcomes Delivered

- Prioritized findings with severity ratings
- Demonstrated attack paths that show how multiple weaknesses can be chained
- Prescriptive remediation guidance that engineering teams can act on
- Strategic recommendations for eliminating entire classes of vulnerabilities earlier in the product lifecycle

Why It Matters

PSRs move beyond surface-level vulnerability scanning. By combining hardware, software, and ecosystem testing, our methodology provides security leaders with a holistic view of risk and a clear plan for remediation that balances engineering effort with business impact.

ABOUT BISHOP FOX

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments.

L□□□□ □ O□□ □□ BISHOPFOX.COM