Kiteworks

SOLUTION BRIEF

Kiteworks Secure Data Forms Hardening

Reduces 123FormBuilder CVSS Score From 9.4 to 7.6

Overview

A recent discovery of two SQL injection vulnerabilities in the shared codebase underlying 123FormBuilder and Kiteworks Secure Data Forms (SDF) vividly illustrates the security advantages of the Kiteworks platform. Both vulnerabilities, filed together under CVE-2026-24782, scored 9.4 (Critical) on the 123FormBuilder SaaS platform. On Kiteworks SDF, the same findings scored only 7.6 (High), a direct result of the platform's layered hardening measures, rearchitected sensitive data storage, and single-tenant deployment model. Organizations using Kiteworks SDF can trust that these built-in protections substantially reduce the business risk of data breaches, unauthorized access, and regulatory noncompliance.

Discovered and Responsibly Disclosed

Two closely related SQL injection vulnerabilities were discovered by two external security researchers working together through the Kiteworks bug bounty program for Secure Data Forms. Given the shared codebase, Kiteworks security engineers confirmed that 123FormBuilder was affected as well. Due to their similarity, the vulnerabilities were consolidated into a single CVE entry, CVE-2026-24782, filed by Kiteworks for the SDF product. In keeping with Kiteworks' commitment to responsible disclosure and consistent with the CISA Secure by Design pledge Kiteworks has signed, findings were promptly assessed, triaged, and remediated across both product lines, with proactive customer communication throughout.

Critical Vulnerabilities With Potentially Severe Impact — On 123FormBuilder

On the 123FormBuilder SaaS platform, both vulnerabilities received a CVSS score of 9.4, placing them firmly in the Critical category. The elevated score reflects several compounding factors:

- **Network-accessible attack surface:** The vulnerabilities are reachable over the network without authentication requirements that would meaningfully constrain exploitation.
- **Shared infrastructure:** As a multi-tenant SaaS environment, a successful attack against 123FormBuilder's platform could potentially expose data belonging to multiple unrelated organizations simultaneously.

Solution Highlights

- **Safer Data Storage**
- **Risk Reduced by Design**
- **No Cross-Tenant Exposure**
- **Audit-Ready Compliance**

- **Unrestricted data access:** Submitted form data, which frequently includes personally identifiable information (PII), financial data, and other sensitive data, is stored in a manner directly accessible to the application layer, and therefore reachable via SQL injection.

The combination of these factors drives both a high exploitability sub-score and a high impact sub-score under CVSS methodology, resulting in the 9.4 Critical rating.

Kiteworks treated this with the urgency it warranted. Within our 7-day SLA for Critical vulnerabilities, our engineering team investigated the root cause, developed and verified a fix, completed full QA validation, and rolled out the patch to the 123FormBuilder SaaS environment, all without disruption to customer operations.

Severity Reduced to 7.6 by the Kiteworks Hardened Appliance

On Kiteworks Secure Data Forms, the same two vulnerabilities were assessed at 7.6, High severity rather than Critical. This reduction is the direct result of multiple independent hardening layers that together constrain both exploitability and potential impact. Because 7.6 falls within Kiteworks' High severity SLA, the patch was delivered comfortably within that window as part of the regular SDF release cycle, with full QA and no emergency intervention required.

Hardened Virtual Appliance

The Kiteworks hardened virtual appliance provides a defense-in-depth foundation that SDF inherits fully. This includes:

- A secure build process and continuous vulnerability management
- A minimized attack surface with perimeter protection
- An embedded network firewall and intrusion detection system
- Strong encryption for data in transit and at rest
- An embedded Web Application Firewall (WAF), automatically updated by Kiteworks threat intelligence and requiring no maintenance from the customer

The WAF is tuned to the specific traffic patterns of the Kiteworks Private Data Network (PDN), and is capable of identifying and blocking exploitation attempts for known attack classes, including SQL injection, before they reach the application layer.

Rearchitected Storage of Sensitive Data

Beyond the appliance-level hardening SDF inherits, Kiteworks engineers rearchitected how SDF stores submitted form data, the most sensitive category of information a forms platform handles. This restructuring places sensitive submission data outside the direct reach of several categories of vulnerabilities, including the SQL injection vectors identified in CVE-2026-24782. As a result, even a successful exploitation of these vulnerabilities would not have exposed submitted form data, a fact that directly reduced the impact sub-score and contributed meaningfully to the drop from 9.4 to 7.6. Even in a scenario where an attacker partially exploited the vulnerability, the data accessible to them would be substantially constrained compared to what is exposed in the 123FormBuilder architecture.

Single-Tenant Deployment

Unlike 123FormBuilder, which operates as a shared SaaS platform, Kiteworks Secure Data Forms runs in a dedicated single-tenant environment for each customer. This architectural separation means there is no risk of cross-customer data exposure. An attacker targeting one organization's SDF instance has no path to any other organization's data, an inherent and unconditional guarantee that multi-tenant SaaS platforms simply cannot provide.

Why Critical Is a Different Threat Category, Not Just a Higher Number

The difference between a Critical and a High vulnerability is commonly underestimated when viewed as a simple point gap on a 0–10 scale. In practice, the distinction reflects a fundamentally different threat profile, and the gap in real-world exploitability is considerably wider than the numbers alone suggest.

Critical vulnerabilities, by definition, combine a highly accessible attack vector with low complexity and very low privilege requirements. This makes them the primary target class for opportunistic attackers, automated exploit tools, and ransomware operators. Threat intelligence data bears this out starkly: analysis of dark web forum activity found that Critical-rated vulnerabilities are discussed and traded at more than double their share of the overall CVE population, approximately 25% of dark web vulnerability references versus only 12% of all published CVEs. This reflects the disproportionate interest threat actors place on this category1. These are the findings that get weaponized into standalone, scalable attack campaigns.

High-severity vulnerabilities, while serious and requiring timely remediation, occupy a materially different threat model. Their defining characteristic, captured in industry severity frameworks, is that they are typically difficult to exploit, requiring an attacker to chain them with other vulnerabilities, leverage a pre-existing foothold, or operate under specific environmental conditions2. CISA has explicitly noted this chaining dynamic: attackers frequently use lower-scored vulnerabilities as steppingstones, combining them incrementally to escalate privileges and achieve their objectives3. A High vulnerability in isolation, without the supporting conditions or complementary weaknesses needed to complete the chain, rarely translates into a standalone breach.

This means the reduction of CVE-2026-24782 from 9.4 (Critical) on 123FormBuilder to 7.6 (High) on Kiteworks SDF represents a much larger practical security improvement than the 1.8-point numerical gap implies. On 123FormBuilder, these vulnerabilities represented a realistic, standalone attack path requiring no special conditions or chaining. On Kiteworks SDF, the same underlying weaknesses are constrained to a threat model that requires an attacker to overcome multiple independent hardening layers, operate within a single-tenant environment, and construct a multi-stage exploit chain, moving the vulnerability firmly out of the category that drives the vast majority of real-world breaches.

123FormBuilder Customers Deserve the Protection of Kiteworks SDF

Organizations currently using 123FormBuilder can migrate to Kiteworks Secure Data Forms and immediately benefit from the same familiar functionality they rely on today, while gaining the full protection of the Kiteworks hardening stack. Key advantages include:

- **Substantially reduced vulnerability severity:** The hardening measures already demonstrated here reduced a 9.4 Critical finding to a 7.6 High, with ongoing security investment continuing to improve that posture over time.
- **Single-tenant isolation:** No shared infrastructure means no shared risk. Ever.
- **Tiered, SLA-driven response:** Critical findings on 123FormBuilder are patched within 7 days. The same vulnerabilities on SDF qualify as High, enabling remediation within the regular release cycle without emergency procedures or operational disruption.
- **Comprehensive audit logging:** Centralized, tamper-evident logs support compliance obligations and continuously feed SecOps workflows.
- **Unified policy control:** SDF is part of the Kiteworks Private Data Network (PDN), enabling consistent governance across file sharing, email, upload forms, SFTP, managed file transfer (MFT), and API integrations.

Kiteworks Secure Data Forms is not merely a repackaged forms product. It is a hardened, enterprise-grade platform built to handle sensitive data with the security posture that modern compliance and risk management requirements demand.

References

[1] S2W Blog, “Detailed Analysis of Recent Vulnerability Trends and Attack Patterns” (December 2025) – medium.com/s2wblog

[2] Atlassian, “Severity Levels for Security Issues” – atlassian.com/trust/security/security-severity-levels

[3] Balbix, “Analyzing CISA Known Exploited Vulnerabilities” – balbix.com/blog/analyzing-cisa-known-exploited-vulnerabilities-with-business-context