PSPDFKit SDK
Security and Privacy

How PSPDFKit Protects Our Customers and Their End Users

01

Purpose and Intended Audience

This white paper is aimed at decision-makers who work for companies that are in the process of choosing a trusted technology partner for PDF processing, manipulation, and rendering. Whether you have a custom web, desktop, server-based, or mobile application, we understand that managers and decision-makers need to be aware of the implications of the security practices of their chosen PDF SDK.

Enterprise-grade software security is like a chain, and time has proven that when you're embedding another technology into your own, you are only as strong as your weakest link.

In this whitepaper, we'll address why we're proud to state that we're the most secure PDF SDK in the industry. In case you're unfamiliar with security terms and terminology, this document will take you step-by-step to understand the HOW and the WHY we handle security within our company, our products, and our services.

02

Security Should Be the Top Priority When Evaluating a PDF SDK

By the Numbers

13%
of data breaches are caused by third-party software (source: IBM)

41%
year-over-year growth of ransomware attacks (source: IBM)

64%
of CISO's say data theft of destruction is their top concern (source: Fortra)

62%
of companies say their security team is understaffed (source: IBM)

70%
more account breaches in Q3 compared to Q2 (source: surfshark)

6th
most common attack vector is third-party components (source: OWASP)

It's absolutely paramount that the security practices and history of a PDF SDK provider should be carefully scrutinized before embedding into your own software products and services. This year, an independent report from IBM states that ransomware attacks have increased 41% year by year, and Surfshark reports that account breaches increased 70% quarter-over-quarter.

Sophisticated attackers use tried-and-true methods in order to perform a security breach, or to elevate their privileges while executing a cyber-security attack. These tried-and-true methods are known as **Attack Vectors**. One of the most common Attack Vectors is to use hidden vulnerabilities in third-party SDKs/libraries in order to remotely execute malicious code.

In 2021, OWASP, the international security foundation dedicated to security assessments and research, stated that Attack Vectors using vulnerable and outdated third-party components in software is the **6th most common web application security risk**. Just a few years ago back in 2017, it was the 9th most common. According to a 2022 study by IBM, 1 in 8 data breaches are caused by third-party software.

Company CISOs (Chief Information Security Officers) are very concerned about these trends, because embedding an insecure PDF SDK is an unacceptable risk.

03

The Impact of an Insecure SDK

When it comes to enterprise-grade security, the stakes are high. The long-tail costs of a data breach can extend for months and years and include significant ongoing expenses. These costs include lost data, business disruption, revenue losses from system downtime, notification costs (providing a timely advisory to your impacted customers), and damage to your brand's reputation.

What Is the Total Cost of a Vulnerability?

$9.44
million

284
days

15%
share price

Before deciding to partner with a PDF SDK provider, it's important to understand that the license fee that you pay is not the TCO (total cost of ownership).

IBM's latest public report on the costs and impact of a security breach in 2022 states that the average cost of a breach is a staggering **USD $9.44 million**. Additionally, after a security breach has occurred, the report states that the average time to identify, assess, and contain a breach is **284 days**. Now, for publicly traded companies, there's an additional cost to account for. After a security breach has been made public, the average NASDAQ share price of the affected company **drops over 15%**.

If your chosen PDF SDK provider is unwilling or unable to fix a publicly disclosed software vulnerability, then your customers are left exposed to malicious exploits and targeted

cybersecurity attacks. As a result, the cost and expense of finding, fixing, and responding to an active security breach is a major component of the total cost of ownership for a PDF SDK.

However, the highest cost is associated with litigation that often follows data breaches, for instance:

- CVE-2017-5638 led to the infamous Equifax breach of 2017 that cost the company $425 million to settle the class action lawsuit. (source: FTC)

- A GOP data firm that exposed millions of Americans' personal information faced a class-action lawsuit for the first time, arguing that the "actual damages" exceed $5 million. (source: Business Insider)

- A lawsuit filed against Facebook alleged that the company was guilty of unlawful business practices, deceit by concealment, negligence, and violations of California's Customer Records Act as a result of a massive hack that exploited a security flaw to steal account credentials of as many as 50 million users. (source: The Verge)

- Three years after Neiman Marcus disclosed that it had become the victim of a hack attack in 2013, exposing the credit card information of more than 350,000 customers, the retailer reached a $1.6 million settlement in the subsequent class action lawsuit. (source: Consumerist)

- Target Corp agreed to pay $39.4 million to resolve claims by banks and credit unions that said they lost money because of the retailer's late 2013 data breach. This settlement resolved class-action claims by lenders seeking to hold Target responsible for their costs to reimburse fraudulent charges and issue new credit and debit cards.
(source: Reuters)

04

Impact Studies: Real World Examples of the Results of Incorporating an Insecure PDF SDK

PSPDFKit was founded in 2011, and has been providing secure, stable, and reliable PDF SDKs (and software services) for enterprises, governments, and small businesses. We have over 500 million users worldwide, and our track record speaks for itself: we have had zero reported security incidents against our PDF SDK since Day-1. Think about that for a moment.

Reported security incidents (also called CVEs), are Common Vulnerabilities and Exposures, and are reported and cataloged by NIST in the National Vulnerability Database.

Unfortunately, a leading competitor in the span of 13 consecutive months has had over 11 reported security vulnerabilities (CVE's) reported against their PDF SDK.
Let's examine the results of publicly reported CVEs on two multinational software companies that have been impacted by incorporating an insecure PDF SDK.

IMPACT STUDY #1 →

Autodesk

Autodesk is the household name for making CAD software and services for the automotive, engineering, architecture, construction, and manufacturing industries. They have publicly disclosed that the use of the PDF SDK from a leading competitor has resulted in wide-spread security vulnerabilities in 17 of their software products. According to the disclosures, these vulnerabilities have existed for over four years and affect various Autodesk software products running on PC and MacOS operating systems. Affected products include Autodesk's well-known AutoCAD software as well as their Revit and Navisworks tools.

This year, two separate reports from Autodesk updated in April and July, both with high severity state that Autodesk's software can be exploited to execute arbitrary code through any of the 6 vulnerabilities listed below:

HIGH

A maliciously crafted PDF file may be used to dereference a pointer for read or write operation while parsing PDF files in Autodesk Navisworks 2022. The vulnerability exists because the application fails to handle a crafted PDF file, which causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code.

[**CVE-2022-27872**]

HIGH

Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using [*A Leading Competitor*] prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code.

[**CVE-2022-27871**]

HIGH

A Memory Corruption vulnerability may lead to code execution through maliciously crafted DLL files.

[**CVE-2022-27527**]

HIGH

A maliciously crafted PDF file can be used to dereference for a write beyond the allocated buffer while parsing [*A Leading Competitor*] files. The vulnerability exists because the application fails to handle a crafted [*A Leading Competitor*] file, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code.

[**CVE-2022-25795**]

HIGH

A Memory Corruption vulnerability may lead to code execution through maliciously crafted DLL files through [*A Leading Competitor*] earlier than 9.0.7 version.

[**CVE-2021-40161**]

HIGH

[*A Leading Competitor*] prior to 9.0.7 version may be forced to read beyond allocated boundaries when parsing a maliciously crafted PDF file. This vulnerability can be exploited to execute arbitrary code.

[**CVE-2021-40160**]

As a result, a sophisticated attacker can use Autodesk software to attack any of the corporate/personal computers owned by the millions of Autodesk customers.

Also stated in both reports, Autodesk has acknowledged that some versions of their products before 2021 will not be patched/fixed against some of the disclosed vulnerabilities.

IMPACT STUDY #2 →

M-Files

M-Files is a Document Management Platform which leverages metadata in order to enable their customers to manage their documents and information. M-Files utilizes a PDF SDK from a leading competitor and has publicly reported (also in 2022) that their Hubshare product/service has included a severe vulnerability. This vulnerability, when exploited, enables unauthenticated attackers to access restricted PDF files and bypasses any and all security authorization schemes.

The security report on the M-Files website states:

"[*A Leading Competitor*] doesn't provide any native mechanism to ensure that rendered documents cannot be opened by someone else [other] than the user supposed to access the rendered document. We had to implement our own additional layer of security to check for the current user session and determine if the URLs can be opened or not."

Below is a list of the vulnerabilities:

HIGH

Broken access controls on [*A Leading Competitor*] WebviewerUI in M-Files Hubshare before 3.3.11.3 allows unauthenticated attackers to upload malicious files to the application server.

[**CVE-2022-39019**]

HIGH

Broken access controls on [*A Leading Competitor*] data in M-Files Hubshare before 3.3.11.3 allows unauthenticated attackers to access restricted PDF files via a known URL.

[**CVE-2022-39018**]

HIGH

Javascript injection in [*A Leading Competitor*] in M-Files Hubshare before 3.3.10.9 allows authenticated attackers to perform an account takeover via a crafted PDF upload.

[**CVE-2022-39016**]

HIGH

A use after free vulnerability was discovered in [*A Leading Competitor*] SDK version 9.2.0 A crafted PDF can overwrite RIP with data previously allocated on the heap. This issue affects: [A Leading Competitor] SDK on 9.2.0 on OSX; 9.2.0 on Linux; 9.2.0 on Windows.

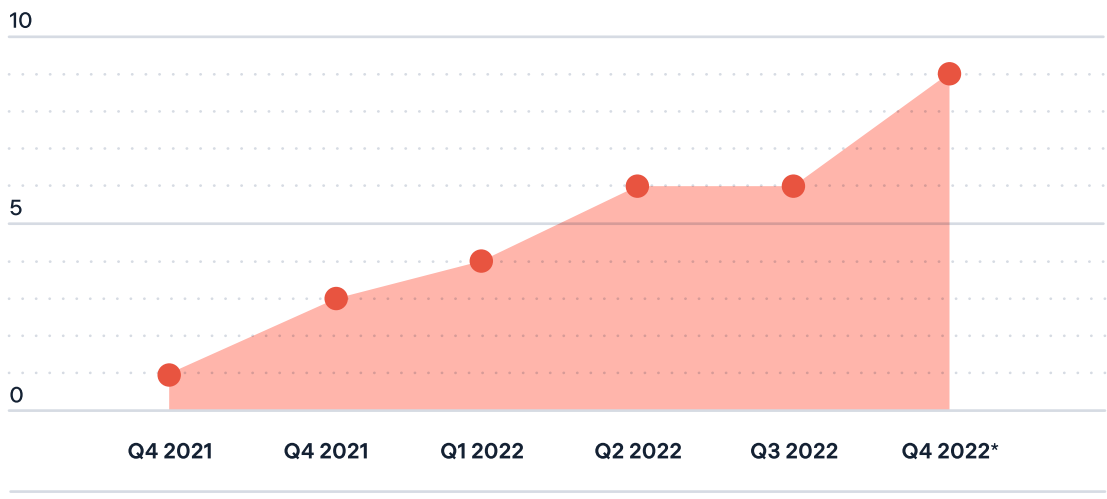
[**CVE-2022-24960**]

MEDIUM

[*A Leading Competitor*] WebViewer UI 8.0 or below renders dangerous URLs as hyperlinks in supported documents, including JavaScript URLs, allowing the execution of arbitrary JavaScript code.

[**CVE-2021-39307**]

Both Autodesk and M-Files have stated in their reports that the security vulnerabilities within their own software products existed due to the security vulnerabilities of their chosen PDF SDK provider.



*On Nov 30, 2022

(source: National Vulnerability Database)

05

The PSPDFKit Approach to Security

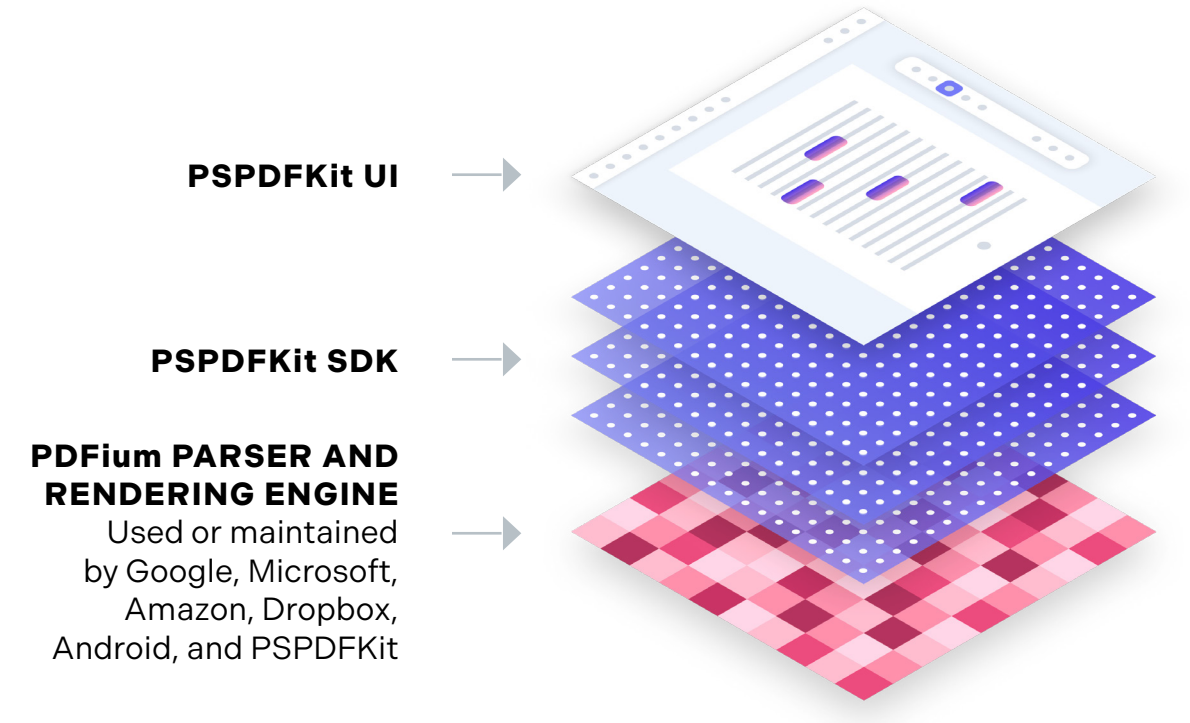
Far from being an afterthought, or the focus of occasional initiatives, security is tightly integrated into the way PSPDFKit operates.

Start With a Secure PDF Engine

TRILLIONS
of PDFs

BILLIONS
of users

The PSPDFKit core SDK and user interface sit on top of an optimized fork of PDFium, which is the same secure PDF engine used by the Chrome web browser and Android mobile devices. PDFium's security is managed by Google's Chromium security team, and has code contributions from companies like Microsoft, Dropbox, and PSPDFKit. PDFium is used in countless applications by over 2 billion users to open trillions of PDFs every year. As a result, our PDF engine has been battle-tested to be secure, memory safe, resilient, and very efficient.



“Because PDFium has large stakeholders such as Chromium, downstream users benefit from the significant effort Chromium makes in securing PDFium.”

Jonathan Metzman
Software Engineer, Open Source Security Team, Google

Backed by a Strong Security Culture

- Employee background checks
- Security training for all employees
- Dedicated security officer
- Secure software development lifecycle

Earlier this year, we announced that we have successfully completed the SOC 2 Type 1 Audit. The SOC 2 (Service Organization Control) is a technical audit that measures the security, availability, confidentiality, processing integrity, and privacy of an organization’s data processing systems and determines whether adequate safeguards and controls are in place.

“We’re moving toward an increasingly digital world, and our most sensitive documents are progressively being stored and processed through complex electronic systems, so security is more important than ever.”

Serana Warren
PSPDFKit Information Security Officer

Verified by Independent Third-Parties

In order to ensure top-notch security, we partner with Prescient Security for independent third-party penetration testing of our PDF SDKs and services. This is essential, due to the fact that our enterprise, government, and startup customers expect independent verification of our security and privacy controls.

Additionally, the PDF engine for our PDF SDK (PDFium) is independently tested by ourselves, Google, and other organizations to ensure that PDFs are safely rendered and viewable without being vulnerable to a malicious exploit hidden within the PDF.

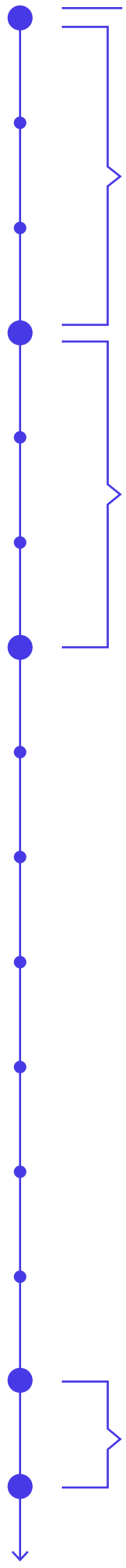
“Open source security is a cooperative effort among software vendors and other community participants. It's not as simple as the oft-repeated ‘With many eyes, all bugs are shallow’ aphorism. But it does mean that an entire software community works on the security of not just a single project or product but also on all the open source code that feeds into it.”

Gordon Hoff
Technology Evangelist at Red Hat

Time is Critical Regarding Security Vulnerabilities

If a security flaw or a vulnerability is found with your chosen PDF SDK, then time is of the essence. As mentioned earlier, the rendering engine for our Open Source SDK is tested by ourselves, Google, and other organizations. The figure below shows how quickly our rapid-response team resolves security issues reported on our rendering engine.

PSPDFKIT SECURITY UPDATE TIMELINE



Day 1

PDFium security bug is fixed by Google

Weeks 1–3

PSPDFKit pulls in the security bug fix

Weeks 4–6

Security bug fix appears in a PSPDFKit release or nightly

Week 14

Security bug is publicly disclosed by Google

Within a 3 week timeframe after a security issue has been resolved, we have already applied the fix to our SDK. Additionally, by Week-6 we have already a version of the fix available for customers to test and implement on their end. And of course, by Week-14 the security issue is publicly disclosed by Google to the public. As contributors to the public Open Source PDFium project, we believe strongly in rapid response, and public disclosure of security bugs and vulnerabilities. Therefore, as a result, we are able to fix issues BEFORE they become a CVE in the National Vulnerability Database, and our customers (and their clients) stay safe and secure.

Conversely, a leading competitor has public vulnerabilities that have been open and exposed to the public for months, and some of the unmitigated vulnerabilities continue to impact their customers. For instance, Autodesk has acknowledged that due to the fact that the vulnerabilities continue to exist, older versions of their software are not recommended to be used by their users. The Autodesk report states:

- Updates are not available for previously supported versions of Autodesk® Inventor and AutoCAD® – versions 2021-2019.
- An update is not available for 32bit AutoCAD 2019

— source: Autodesk.com

Additionally, the disclosure report from M-Files clearly states that:

“We had to implement our own additional layer of security to check for the current user session and determine if the URLs can be opened or not.”

— source: M-Files.com

Therefore, if your PDF SDK provider is unwilling (or unable) to resolve security issues or vulnerabilities, then the security implications fall squarely on your shoulders.

06

Zero vs 11: and Why It’s Important

At PSPDFKit, Enterprise-Grade Security is literally a part of everything that we do. Our PDF SDKs are built upon an iron-clad secure PDF Engine, which is Open Sourced to the public, and tested and used by Google. We have a strong security culture in our corporate DNA, and this is reflected in the products and services we provide for our customers. Finally, our PDF SDK is verified by Independent Third-Parties.

Whereas other PDF SDK providers may be comfortable with licensing their software containing 11 (discovered) security vulnerabilities, we have a proven track record **in the lifetime of our company** to have absolutely zero CVEs registered against our software SDKs and services. The cost of researching, assessing, testing, and resolving a security vulnerability is a significant part of the TCO for licensing a PDF SDK.

Your PDF SDK provider should be a trusted partner for the success of your business, and not a trojan horse.

SOURCES

Data breaches caused by third-party software

Ransomware attacks

Companies saying their security teams are not sufficiently staffed

CISOs saying that groups that seek to steal or alter our data or assets are their top concerns

CISOs saying that Ransomware or other malware infection that seek to steal data or extort payment pose the greatest danger

More security breaches in Q3 than Q2

Vulnerable and outdated components is a common security risk

Costs of a security breach

Equifax 2017 breach

Equifax breach costs

GOP data firm that exposed millions of Americans' personal information is facing its first class-action lawsuit

Ride-sharing company Uber had to pay a penalty to all 50 states after allegedly concealing a data breach in 2016 that affected roughly 57 million people.

A lawsuit filed against Facebook as a result of a massive hack that exploited a security flaw to steal account credentials of as many as 50 million users.

Neiman Marcus reached a $1.6 million settlement in a class action lawsuit

Target Corp agreed to pay $39.4 million to resolve claims by banks and credit unions that said they lost money because of the retailer's late 2013 data breach

CVE report affecting M-Files (1)

CVE report affecting M-Files (2)

CVE report affecting M-Files (3)

CVE report affecting Autodesk (1)

CVE report affecting Autodesk (2)

CVE report affecting [competitor] SDK

Autodesk's security advisory

M-File's Security advisory

Our SOC 2 type 1 announcement