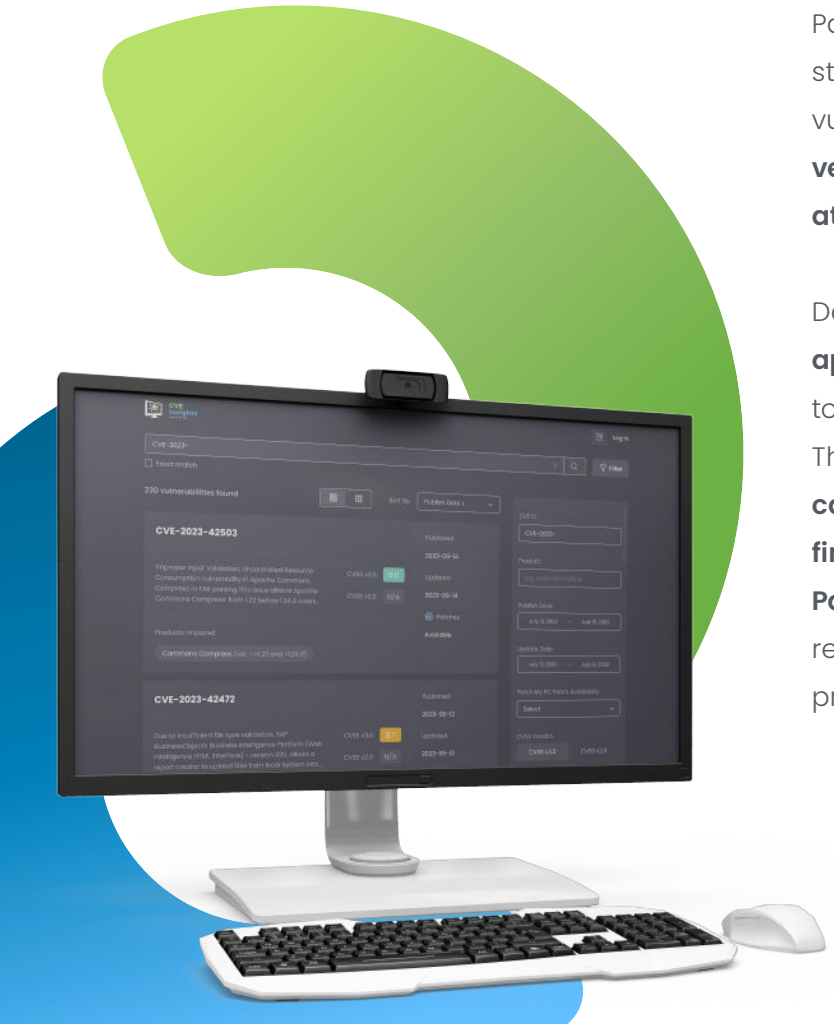
PATCH MY PC

Patch Now or Pay Later: The Financial and Security Risks of Neglected Application Updates



Introduction

Patching isn't just about compliance—it's about staying ahead of cyber threats. Unpatched vulnerabilities remain one of the **biggest attack vectors,** with **zero-day exploits and ransomware attacks** often leveraging outdated software.

Despite IT teams' best efforts, **third-party applications** often fall through the cracks, leading to **breaches, compliance failures, and downtime.** This white paper highlights **real-world attacks caused by unpatched software,** explores **the financial and operational risks,** and outlines how **Patch My PC automates remediation** while offering real-time **CVE insights** to help organizations prioritize security.

The True Cost of Delayed Patching

Neglecting software updates isn't just a minor oversight — it's a **major security liability.** A **2023 Verizon Data Breach Report** found that **over 80% of successful cyberattacks** exploited known vulnerabilities that had patches available.

When Patching Fails, Here's What Happens:

- **Zero-Day Exploits** → Attackers use vulnerabilities **before a patch is even released.**
- **Ransomware Infections** → Outdated apps serve as **entry points for ransomware attacks.**
- **Compliance Violations** → **Fines, legal consequences, and reputational damage** (GDPR, NIST, HIPAA).
- **Downtime & Financial Losses** → **Remediation costs, lost productivity, and customer trust erosion.**

Example:

In 2017, **Equifax was breached via an unpatched Apache Struts vulnerability.** The result? **147 million records exposed and a $700M fine.**

These consequences are not hypothetical. They are real-world failures that continue to happen to organizations that fail to patch their systems on time. Let's examine a few more cases where unpatched applications led to major security breaches.

Case Studies: When Unpatched Applications Led to Breaches

Google Chrome (CVE-2022-1096) – Zero-Day Exploited

- **Vulnerability:** A **type confusion bug** in the **V8 JavaScript engine.**
- **Impact:** Attackers **executed arbitrary code** via crafted web pages before a patch was available.
- **Outcome:** Google issued an **emergency update** in **March 2022,** but systems that delayed patching remained vulnerable.
- **Lesson:** **Browsers are a top target**—attackers move **fast,** so patching must be **immediate.**

Mozilla Firefox (CVE-2022-26485) – Remote Code Execution

- **Vulnerability:** A **use-after-free flaw** in **XSLT processing.**
- **Impact:** Attackers **exploited memory corruption** to gain control over victim systems.
- **Outcome:** Mozilla released a **high-priority patch,** but organizations with **manual patching delays remained at risk.**
- **Lesson:** **Even a few days of delay** increases attack exposure.

Adobe Acrobat Reader (CVE-2023-26360) – PDF Exploit in the Wild

- **Vulnerability:** A flaw enabling **arbitrary code execution** via **malicious PDFs.**
- **Impact:** Hackers used **crafted PDFs in phishing attacks** to install malware.
- **Outcome:** Adobe **patched it quickly,** but unpatched users faced **data theft and system compromise.**
- **Lesson:** PDF readers are **high-risk** since **users regularly open external documents.**

Zoom Client for Meetings (CVE-2022-22784) – Chat-Based Exploit

- **Vulnerability:** **Remote code execution via malicious chat messages.**
- **Impact:** A **single unpatched client** could allow attackers to **control a machine remotely.**
- **Outcome:** Zoom **fixed it,** but organizations that failed to update **remained vulnerable to remote takeovers.**
- **Lesson:** **Collaboration apps a re high-value targets**—patch them aggressively.

7-Zip (CVE-2022-29072) – Privilege Escalation Attack

- **Vulnerability:** A **local privilege escalation flaw** in **.7z file handling.**
- **Impact:** Hackers could **gain admin privileges** and **execute arbitrary commands.**
- **Outcome:** A patch was released, but **attackers exploited systems that delayed deployment.**
- **Lesson:** **Even non-critical apps** can serve as **stepping stones for attacks.**

Download our ROI calculator and find out how much you can save

Competitive Landscape: How Companies Handle Patching Today

With the risks clearly demonstrated, the question becomes: **How are organizations handling patching today?** To understand why automation is essential, let's compare **manual patching, native tools, and Patch My PC:**

Approach	Pros	Cons
Manual Patching	Full control over patch timing	Labor-intensive, high risk of delays and human error
Native Tools (SCCM, Intune)	Centralized Windows patching	Limited third-party app coverage, requires manual packaging and deployment
Patch My PC	Automated, scalable, security-driven	None: fully automates patching and integrates seamlessly with Intune & SCCM

Key Takeaway: As the table highlights, manual patching and built-in tools **fail to scale and protect against zero-day exploits.** Patch My PC closes the gap by automating updates across Windows and third-party apps, ensuring patches are applied efficiently and securely.

The Role of Patch My PC in Mitigating Risks

As we've seen, relying on manual patching or native tools alone leaves significant security gaps. This is where **Patch My PC comes in.**

How Patch My PC Improves Security:

- **Automates third-party app updates** across **SCCM & Intune.**
- **Ensures patches are applied immediately,** eliminating delays.
- **Provides compliance reporting** to verify all devices are up to date.
- **NEW: CVE Insights** – Gain real-time visibility into **which vulnerabilities apply to your environment,** their **severity,** and actionable remediation steps.

Why CVE Insights Matters:

- **Proactive Risk Management** – Having visibility into **which CVEs affect your environment** helps organizations stay ahead of threats.
- **Efficient Patch Prioritization** – Knowing which vulnerabilities are **actively exploited** ensures the most **critical updates are applied first.**
- **Automation and Intelligence** – Patch My PC's integration of CVE Insights **not only identifies risks but also automates remediation,** reducing manual workload for IT teams.
- **Improved Compliance & Reporting** – Organizations can **demonstrate regulatory compliance** by ensuring security patches align with industry frame- works like **NIST, ISO 27001, and CIS Benchmarks.**

No more guessing. No more manual patching.
Just security-driven automation.

Download our free app and instantly gain insights around the newest CVE's and how they impact your organization.

Best Practices for Enterprise Patch Management

Patching needs **a proactive strategy.** Here's how organizations can ensure **continuous protection:**

4-Step Strategy for Patching Success

1. **Adopt an "Auto-Patch" Mindset** – Automate updates to **eliminate human error and patching delays.**
2. **Prioritize High-Risk Apps** – Focus on **browsers, document readers, and communication tools** first.
3. **Monitor & Enforce Compliance** – Regularly audit **patch status across all endpoints.**
4. **Implement Update Rings for Phased Deployment** – Use **controlled rollout rings** (Pilot, Broad, Critical) to **test updates before full deployment.**

Conclusion: Patch Now or Risk a Breach

The data is clear: **delaying patches creates a security risk.** Recent breaches prove that even well-known applications like Chrome, Firefox, and Adobe Reader can be exploited **within days** of a vulnerability being disclosed.

Automated patching solutions like **Patch My PC** remove the guesswork, **ensuring vulnerabilities are patched before they become a threat.**

Ready to automate pitching today?

Scan to book a demo.

Resources

1. Google Chrome (CVE-2022-1096) – Zero-Day Exploited

- **Source:** National Vulnerability Database (NVD) entry for CVE-2022-1096
- **Link:** https://nvd.nist.gov/vuln/detail/CVE-2022-1096

2. Mozilla Firefox (CVE-2022-26485) – Remote Code Execution

- **Source:** Mozilla Foundation Security Advisory 2022-09
- **Link:** https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/

3. Adobe Acrobat Reader (CVE-2023-26360) – PDF Exploit in the Wild

- **Source:** CISA Advisory on Adobe ColdFusion CVE-2023-26360
- **Link:** https://www.cisa.gov/news-events/alerts/2023/03/15/adobe-releases-security-updates-coldfusion-resolve-cve-2023-26360

4. Zoom Client for Meetings (CVE-2022-22784) – Chat-Based Exploit

- **Source:** Zoom Security Bulletin
- **Link:** https://explore.zoom.us/en/trust/security/security-bulletin/

5. 7-Zip (CVE-2022-29072) – Privilege Escalation Attack

- **Source:** National Vulnerability Database (NVD) entry for CVE-2022-29072
- **Link:** https://nvd.nist.gov/vuln/detail/CVE-2022-29072

6. 2017 Equifax Breach via Apache Struts Vulnerability

- **Source:** Equifax's official statement on the cybersecurity incident
- **Link:** https://www.equifaxsecurity2017.com

CVE Insights
PATCH MY PC