

AN ARXNIMBUS POSITION PAPER

THE DEBT CAME DUE

What Black October revealed about pricing
the decision to go dark

71%

OF PHP INSTALLATIONS IN QUALYS'S CUSTOMER BASE RUN END-OF-LIFE BRANCHES.

Most will never receive an official patch. When PHP2Shell hit, the question for most enterprises wasn't "patch." It was upgrade, isolate or retire, and what each would cost.

The Debt Came Due:

What Black October Reveals About Pricing the Decision to Go Dark

By R. David Moon, CEO & Co-Founder, and Andrew Patterson, COO · ArxNimbus · As of October 27, 2026

The thesis in one line. Black October exposed a gap in translation, not in detection. Scanners found vulnerable PHP within hours. What organizations lacked was a common financial denominator for the expensive, binary decisions they had to make across thousands of assets in a matter of hours: patch, isolate, take offline or migrate off end-of-life software.

Behind those decisions sat two debts most organizations had never priced: **technology debt**, what they had not modernized, and **security debt**, what they had not secured, in old technology and new. In one week, both came due.

1 Black October was a week when many accounts came due at once.

The event itself is smaller and messier than its label. “Black October” is a social-media name for a cluster of security disclosures that peaked between October 19 and 22, 2026. The centerpiece is PHP2Shell, two critical unauthenticated remote code execution flaws in the PHP interpreter itself (CVE-2026-109618 and CVE-2026-109619). It was a core-runtime vulnerability, not a compromise of php.net, PECL or Packagist.

The label also hides the clock. Several underlying attacks began weeks or months earlier: a breach of California student data ran from May to September, the weak certificate authority keys at the center of one incident date to an April 2025 key ceremony, and a Palo Alto PAN-OS flaw (CVE-2026-0257) has been exploited since May. Read it as a run of old bills arriving together, not one coordinated campaign.

Five foundations, one week. PHP2Shell did not arrive alone. Between October 17 and 22, serious flaws landed in five pieces of shared infrastructure that sit underneath most enterprises:

Foundation	Severity	What happened
PHP interpreter (PHP2Shell)	CVSS 9.2	Unauthenticated remote code execution in the runtime behind most of the web; every release back to 5.4 affected.
GitLab (CVE-2026-110264)	CVSS 10.0	Unauthenticated remote code execution in self-managed GitLab, spanning about 12 years of releases. The pipeline that builds everything, AI models and agents included, was itself exposed.
Node.js (CVE-2026-111497)	High	Out-of-bounds write in the Brotli decoder enabling remote code execution in the 22, 24 and 26 release lines.
Unbound DNS (CVE-2026-97206)	CVSS 7.5	Use-after-free in DNS-over-QUIC allowing a remote crash of the resolver.
Certificate infrastructure	Distrusted	Browsers stopped trusting eight intermediate keys from one certificate authority after they proved trivially weak (one was the number “4”).

Different bugs, the same week, all in shared foundations rather than application code. None of them is code an enterprise can review for itself. Whether AI-driven research caused the clustering is not established; the volume of AI-assisted discovery is real, but the certificate failure was a key-management lapse.

71% of PHP installations in Qualys's customer base (12,000 customers, 110 million installs) run end-of-life branches. An independent CybelAngel scan found 59% of 2.24 million internet-facing PHP hosts on versions with no fix coming.

5 serious disclosures in shared foundations in a single week.

32 UK government services taken fully offline as a precaution.

And the dominant measurable loss so far: self-inflicted downtime, not breach.

2 Two debts came due.

Technology debt is the accumulated cost of modernization that was deferred: hardware, software and platforms kept past their supported or economic life. Most boards know it as an IT budget line.

Security debt is the accumulated exposure an organization carries but has not remediated or funded: known flaws left open, assets nobody inventoried, controls never deployed, privileges never revoked, and new technology adopted faster than it could be secured. Most boards have never seen it in dollars.

Black October showed how the two interact. Seventy-one percent of the PHP installations in Qualys's customer base were technology debt, and the moment PHP2Shell was disclosed, they became security debt that could not be paid by patching. No fix is coming for those branches, so the only options were to upgrade, isolate or retire, each with its own cost and downtime profile.

In the same week, a widely used AI gateway was compromised through its release pipeline and its "latest" tags. That was new software with no technology debt at all, yet it carried real security debt: unpinned dependencies and a concentration of credentials for every model provider it connected to. Technology debt reliably creates security debt, but security debt does not require technology debt.

	Older technology	Newer technology, including AI
Technology debt	High. End-of-life runtimes, heavily customized ERP, hardware past vendor support.	Low. Recently bought and still supported.
Security debt	High, and often unpayable by patching. The options are upgrade, isolate or retire.	High and growing. Models, agents, gateways and AI-written code adopted ahead of inventory, provenance and controls.

Much of the debt is inherited. Every shared foundation carries its own debt, and everyone who depends on it inherits that debt. PHP runs 69.3% of websites whose server-side language is known (W3Techs). One multi-tenant backup application held standing OAuth consent across thousands of Microsoft 365 tenants. AI gateways sit between enterprises and every major model provider. Each is a single point of correlated failure across thousands of firms: the aggregation scenario cyber underwriters model and rarely see.

The maintainers are in debt too. The PHP Foundation acknowledged that a lack of resources delayed the fix for a memory flaw first flagged in a 2024 audit. From October 26, curl began handling low- and medium-severity reports in public to cope with the volume. PostgreSQL 19 pulled eight to ten significant features before release, with a core committer citing AI-assisted review that surfaces defects faster than the team can fix them.

And the clock now runs fast. Rapid7's Q3 2026 data shows an average of three days from disclosure to exploitation of high-severity vulnerabilities. PHP2Shell exploitation began before disclosure. AI lowers the

cost and time of every attack, which raises the interest rate on every unpaid debt. Debt that once could be carried for years can now be called with no notice.

3 PHP2Shell: the debt in detail.

Both flaws are memory-safety bugs in how PHP handles out-of-memory and fatal-error conditions, leaving corrupted internal state that a later request reuses. On Apache with `mod_php`, an unauthenticated request can trigger the first before any application code runs. The PHP project rates both at CVSS v4.0 9.2; NVD scores them 9.8 under CVSS v3.1. Two research teams reported them in August using frontier AI models. On October 23, PHP disclosed a separate session-handling flaw (CVE-2026-115560) that the October 21 releases do not fix.

Exploitation preceded disclosure, and it is now confirmed. Amazon Threat Intelligence recorded an exploit attempt against its MadPot honeypots on October 17. Cloudflare saw thousands of attempts in the 10 hours before the announcement and millions afterward. Germany's BSI, the Dutch NCSC, Japanese officials and UK ministers reported no confirmed successful compromise of government systems. On October 26, CISA added both CVEs to its Known Exploited Vulnerabilities catalog, and researchers have since recorded successful shell executions against exposed test systems.

Timeline (UTC)

Date	Event
Aug 11 and 24	Two research teams independently report the flaws to PHP
Oct 17	First exploitation attempt recorded in Amazon MadPot, from anonymized infrastructure
Oct 20, ~15:00	CVE IDs leak on forums and social media. PHP moves the release forward one day. A proof-of-concept video is published by mistake. CERT-EU issues advisory 2026-018
Oct 21, 07:41	Patched container images are published early, which PHP calls an embargo break
Oct 21, 07:43	Cloudflare observes first attacks
Oct 21, 14:00	PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35 released. CISA, NSA, FBI, UK NCSC, CERT-EU, ENISA and Japan urge immediate patching or taking systems offline
Oct 21 to 22	Attempts rise from tens of thousands to millions. Government and bank takedowns. Exploitation in the wild reported
Oct 23	CVE-2026-115560 disclosed
Oct 26	CISA adds both PHP2Shell CVEs to its Known Exploited Vulnerabilities catalog

Embargoes no longer hold. The PHP Foundation blamed a vendor for publishing-built fixes six hours early. That vendor replied that its team had re-found the bugs with a “basic prompt of ‘find bad vulnerabilities in PHP’” and that “people are able to build an exploit in hours without even knowing what the vulnerability is.” Whoever is right, embargo windows can no longer be assumed to hold. Exposure has to be priced from the earliest evidence of exploitation (October 17), not from the advisory date, and auditors and insurers are already shifting their investigation windows accordingly.

The long tail is the debt. WordPress, Drupal, Joomla, Magento, Laravel, Symfony and a dozen other platforms were shown exploitable on vulnerable PHP. Updating the application does nothing, because PHP parses the request before the application loads. PHP also ships embedded in appliances, control panels and Windows software, and CISA warned that its prevalence “may not be directly observable.” Of the 110 million installations in Qualys's data, only 199,000 were patched in the first 12 hours. Fixes exist only for supported branches 8.2 to 8.5, and running workers must be restarted to pick them up. For most enterprises the decision is not “patch” but “upgrade, isolate or retire.”

4 The dominant measurable loss was self-inflicted downtime.

The UK took 32 government services fully offline and four partially. Precautionary takedowns hit Dutch, Finnish, Danish, German, French and Belgian public services, Australia's cyber agency site, several Japanese banks and brokers, and a US HR software provider. Separately, retail analysts estimate that one major European grocer's unrelated October outage cost €120 million to €150 million in revenue, a reminder of what a few days dark costs at scale.

For boards, “take it offline” is a financial decision that needs pricing.

Markets reacted selectively. The clear casualty was the certificate authority whose keys were distrusted: its shares fell by about a third over three sessions against a stated revenue exposure of about 1%, and its board decided to exit the global SSL/TLS business. That is an outsized reaction to a trust failure. Claims of a market-wide “cyber crash” are unsupported; the S&P 500's decline that week was driven by megacaps. No aggregate PHP2Shell loss estimate exists, and any vendor quoting one should be treated with skepticism.

Disclosure clocks are running on uncertain facts. No SEC Form 8-K Item 1.05 filings tied to Black October were found as of October 23. The four-business-day clock runs from the materiality determination, and companies with possible memory-disclosure exposure may not know for weeks whether credentials were read.

Regulators told organizations to go dark. CISA's October 21 alert told organizations unable to patch, or running PHP 8.1 or older, to take PHP systems offline. In the EU, manufacturers have had to report actively exploited vulnerabilities through the Cyber Resilience Act Single Reporting Platform since September 11, 2026, which makes PHP2Shell the first mass-scale test of CRA reporting for products that embed PHP.

Insurers face questions they did not price. At least one major cyber insurer alerted policyholders before disclosure. Trade press called PHP2Shell “close to the scenario cyber underwriters have long modelled.” Three coverage questions are live: whether business interruption responds to a voluntary shutdown without a breach, whether contingent business interruption sublimits cover a host or vendor outage, and how fast the client patched. No reinsurer or modeler has published a loss estimate.

5 AI was an accelerant and a target.

AI played a real role in Black October, but a more specific one than the social-media narrative claims. There was no single “agent swarm.” AI showed up in three ways, and each adds to security debt differently.

As an accelerant on existing flaws. Frontier models found PHP2Shell for defenders and let others re-find it in an evening. Microsoft attributed a campaign against a multi-tenant backup application to a China-state-aligned actor using an open-source agentic framework, with privileged access reached in under three hours in multiple cases. In another campaign, a single operator ran AI agents against more than 1,200 sites, at a reported cost of about \$50 in tokens per breach. AI raises the interest rate on every old debt.

As a target. A popular AI gateway's release pipeline was compromised with stolen OAuth tokens, shipping a credential stealer to about 49,000 downloads. AI provider keys leaked from developer platforms. AI gateways and agent platforms are now high-value credential vaults.

As new exposure in its own right. Agents and third-party apps holding standing, non-interactive privileges are exposures that exist only because AI was adopted. Precision matters here: the documented vector this month was stolen AI coding-assistant sessions plus unpinned dependencies, not assistants autonomously choosing malicious packages.

The governance shift is captured in one line from Microsoft's Satya Nadella: "assume a model is compromised and contain it from the start." That only works if an organization knows which models, agents and gateways it runs, what authority they hold, and which business processes depend on them.

6 Detection worked. Translation didn't.

Major scanning vendors shipped PHP2Shell checks the same day, and one co-discovered the flaws. Finding vulnerable PHP was not the problem. When 71% of installations in Qualys's customer base run end-of-life branches and every finding carries the same CVSS 9.2, a vulnerability list gives no ranking and no basis for the most expensive call executives faced: whether to take revenue-producing services offline.

The questions boards, CFOs, CISOs and underwriters are asking have converged on four:

- Where exactly are we running PHP, including inside vendor products and appliances?
- What does it cost per hour to take each affected service offline, versus the expected loss of keeping it up?
- If credentials were read from memory between October 17 and our patch date, what is our exposure, and is it material?
- Which of our AI gateways, agents and third-party apps hold standing privileges that an agentic attacker could use at machine speed?

Underwriters add a fifth at 1/1 and Q1 renewals: "Show me your time-to-patch, measured from earliest exploitation."

Pricing the decision has been done before. A \$1.46 billion non-profit health system came to ArxNimbus carrying both debts: a third of its technology environment on outdated, high-risk hardware, and a security budget 75% below industry benchmark run by a four-person team. ArxNimbus modeled seven digital-twin scenarios, from budget to hardware, showing which investments cut the most risk per dollar. Once leadership could see the number, the board funded a dollar-ranked plan: security budget tripled, staff doubled and insurance coverage doubled. That is the upgrade, isolate or retire decision, priced before the debt was called.

7 Where ArxNimbus fits.

ArxIQ, powered by the ArxNimbus Thrivaca™ Patented Actuarial AI Engine, prices technology debt and security debt in the same four numbers at every tier: Net Risk Exposure, EBITDA at Risk™, Protectable EBITDA and Annual Accessible Cost Takeout. The board answer and the CISO worklist come from one engine.

- **ArxIQ Standard** sets the financial baseline from external signal and a short questionnaire, with results in minutes once inputs are collected.
- **ArxIQ Elite** measures continuously with every release, Dev through Prod. It inventories software, AI models, agents and releases, prices every finding to the business process it supports, and adds the Enterprise Business Assurance Score and the operational dependency view: if a system or model fails, which processes stop and what it costs.

- **ArxIQ Pro** includes everything in Elite and adds what happens inside the perimeter: sensitive data exposure, active threat telemetry and the security tools you already own. It recalculates in near real time and runs in the cloud, on premises or air gapped.

People are part of the exposure. Black October's credential thefts ran through people: stolen sessions, approved OAuth consents, keys left in the wrong place. ArxIQ measures human factors and behavior, including workforce risk style and population risk, and prices them alongside technology, so the board sees which populations and processes carry the most behavioral exposure. It is an optional add-on to Elite and included in Pro.

Black October failure modes, mapped to ArxIQ

Failure mode	ArxIQ capability	Available in	Honest limit
Hidden runtimes in appliances, control panels and containers	Software, AI model and agent inventory per release, Dev through Prod, plus outside-in discovery of internet-exposed assets	Elite and Pro	Third-party appliances still need vendor component lists
Five foundations at once, two rated CVSS-critical	One dollar-ranked remediation queue across every affected component and the processes it supports	Elite and Pro	Ranking quality depends on how completely components are inventoried
Patch versus take offline	Operational dependency view and Enterprise Business Assurance Score: which processes stop and what it costs	Elite and Pro	Downtime estimates are only as good as the process-mapping inputs
AI gateways and agents holding credentials	Inventory of models, agents and the authority they hold, mapped to processes, with NIST AI RMF and ISO/IEC 42001 controls priced in dollars	Elite and Pro	Shadow AI outside the inventory is estimated, not observed
Credentials stolen through people	Human factors and behavior: workforce risk style and population risk, priced into exposure	Elite add-on; included in Pro	Measures behavioral risk; does not stop a phishing or consent attack
An event unfolding over days	Near real-time recalculation from threat telemetry and your existing security tools; controls measured against observed attacker behavior	Pro	Requires active telemetry integration
Memory disclosure and credential theft	Sensitive data exposure mapping, scoped to the affected window	Pro	Cannot prove whether a read occurred; that is forensics
Board, disclosure committee and insurer	Four-dollar metrics plus a T-Score against NAICS peers; a documented exposure range per process	All tiers	Materiality is a legal judgment and coverage is the insurer's; ArxIQ informs both

Validated against actual events. The Thrivaca engine modeled UnitedHealth Group's exposure at \$7.4B against \$6.872B in actual losses, approximately 310 days before disclosure. Its methodology is NIST-designed, it has been evaluated by U.S. defense organizations, and it is used to underwrite cyber policies for 35%+ of the S&P 500.

ArxIQ quantifies exposure. It does not prevent incidents, and no quantification platform would have stopped PHP2Shell. What it changes is how fast leadership can make the call, and whether that call is made in dollars.

The next PHP is coming. The debt is already on the balance sheet. The only question is whether leadership can see the number before it is called.

Request an Executive Briefing → arxnimbus.com

About this paper. Event facts reflect reporting through October 27, 2026, six days after the core disclosure. Exploitation status, EPSS scores and CVE-2026-115560 are moving targets. Attribution of the backup-application campaign is Microsoft's assessment. Retail loss figures are external estimates. The absence of SEC filings reflects searches, not a full EDGAR review.

Selected sources

- CISA: Critical Vulnerabilities in PHP Require Immediate Patching. <https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching>
- Amazon Threat Intelligence: PHP2Shell exploitation prior to disclosure. <https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-php2shell-exploitation-prior-to-public-disclosure-in-madpot/>
- CERT-EU Security Advisory 2026-018. <https://cert.europa.eu/publications/security-advisories/2026-018/>
- ENISA: Joint statement on critical PHP vulnerabilities. <https://www.enisa.europa.eu/news/joint-statement-on-critical-php-vulnerabilities>
- Qualys: PHP announces critical security release. <https://blog.qualys.com/vulnerabilities-threat-research/2026/10/20/php-announces-critical-security-release-for-two-vulnerabilities>
- Wiz: PHP2Shell PHP RCE. <https://www.wiz.io/blog/php2shell-php-rce>
- The Register: PHP blames Chainguard. <https://www.theregister.com/security/2026/10/22/php-blames-supply-chain-security-biz-chainguard-for-putting-huge-chunks-of-the-web-at-risk/5304611>
- The Register: UK government services offline. <https://www.theregister.com/security/2026/10/22/php2shell-puts-dozens-of-uk-government-services-out-of-service/5304840>
- SecurityToday: Black October, many attacks had been running for months. <https://www.securitytoday.de/en/2026/10/22/black-october-many-attacks-had-been-running-for-months/>
- Forkast: Black October is a disclosure wave. <https://forkast.news/black-october-is-a-disclosure-wave-the-label-hides-the-clock/>
- Dark Reading: 'PHP2Shell' Bugs Signal Red Alert for Security Industry. <https://www.darkreading.com/application-security/php2shell-bugs-red-alert-security-industry>
- Cybersecurity Dive: China-nexus actor attack on ConnectWise Cloud Backup. <https://www.cybersecuritydive.com/news/china-nexus-actor-attack-connectwise-cloud-backup/833727/>
- Chainguard: LiteLLM 1.107.0 malicious wheels. <https://www.chainguard.dev/unchained/litellm-attacked-again-malicious-1-107-0-wheels-on-pypi-and-docker-hub-october-2026>
- Dark Reading: Hackers abuse AI pen-test tool Cairn. <https://www.darkreading.com/cyberattacks-data-breaches/hackers-abuse-ai-pen-test-tool-cairn>
- Bleeping Computer: Browsers block eMudhra CA certificates. <https://www.bleepingcomputer.com/news/security/mozilla-google-apple-block-compromised-emudhra-ca-certificates/>
- SecurityOnline: Node.js October 2026 security release. <https://securityonline.info/nodejs-security-release-october-2026/>
- Debian Security Tracker: CVE-2026-97206. <https://security-tracker.debian.org/tracker/CVE-2026-97206>
- Insurance Business: NSA warns of critical website flaw. <https://www.insurancebusinessmag.com/us/news/cyber/nsa-warns-of-critical-website-flaw-as-wikipedia-european-government-websites-taken-offline-594432.aspx>
- Axios: PHP vulnerability security update. <https://www.axios.com/2026/10/22/php-vulnerability-security-update-websites>
- CISA: CISA Adds Two Known Exploited Vulnerabilities to Catalog (Oct. 26, 2026). <https://www.cisa.gov/news-events/alerts/2026/10/26/cisa-adds-two-known-exploited-vulnerabilities-catalog>
- The Register: CISA confirms PHP2Shell under attack as researchers clock successful exploits. <https://www.theregister.com/cyber-crime/2026/10/27/cisa-confirms-php2shell-under-attack-as-researchers-clock-successful-exploits/5305681>
- BleepingComputer: GitLab warns of new max severity code execution vulnerability. <https://www.bleepingcomputer.com/news/security/gitlab-warns-of-new-max-severity-code-execution-vulnerability/>
- CybelAngel: 2.24M internet-facing PHP hosts, 59% on versions with no fix coming. <https://cybelangel.com/blog/critical-php-rce-vulnerabilities-cve-2026-109618-and-cve-2026-109619/>
- W3Techs: Usage statistics of PHP for websites. <https://w3techs.com/technologies/details/pl-php>
- Rapid7: Q3 2026 threat update, attackers exploiting vulnerabilities within 3 days. <https://www.rapid7.com/blog/post/tr-q3-2026-threat-update-attackers-exploiting-vulnerabilities-within-3-days/>

- ITdaily: PHP Foundation angered by ‘clumsy’ disclosure of vulnerabilities. <https://itdaily.com/blogs/software/php-angry-clumsy-announcement/>
- The Register: curl to handle low- and medium-severity reports in public. <https://www.theregister.com/a/5304198>
- ActuaIA: PostgreSQL 19 drops 8 to 10 features, per a committer. <https://www.actuia.com/actualite/postgresql-corrige-44-failles-en-2026-contre-7-en-2025-sa-version-19-perd-8-a-10-fonctions-selon-un-committer/>
- Business Today: eMudhra shares take three-day fall to 34%. <https://www.businesstoday.in/markets/stocks/story/emudhra-shares-plunge-14-take-three-day-fall-to-34-heres-why-562965-2026-10-22>
- IamExpat: Albert Heijn faces €150 million sales hit after cyberattack. <https://www.iamexpat.nl/expat-info/dutch-news/albert-heijn-faces-150-million-sales-hit-after-cyberattack>
- Fast Company: Satya Nadella on assuming AI models are compromised. <https://www.fastcompany.com/91623061/ai-model-emergency-brake-or-architectural-demotion>

About ArxNimbus

ArxNimbus was built on a simple idea: AI and actuarial modeling, together, are the most reliable way to measure exposure in financial terms. Since 2017, we have used AI to normalize fragmented security data and actuarial science to quantify its financial impact, producing a continuous, defensible system of record for enterprise exposure.

Built in collaboration with leaders across national security, academia and industry, including MITRE, the University of Chicago and the U.S. Department of Defense, the ArxNimbus **Thrivaca™** Patented Actuarial AI Engine reflects how risk is actually modeled and validated in the real world. **ArxIQ** applies that engine to converged cyber and AI exposure, bringing insurer-grade financial rigor to the decisions that span both.

About the authors

R. David Moon, Chief Executive Officer & Co-Founder. R. David Moon is a quant-focused cybersecurity risk specialist whose career spans Fortune 500 CIO and CISO roles, a Big Four consulting partnership, and senior software-industry leadership. A CISSP and four-year U.S. Air Force veteran with Secret clearance, he brings a 20-plus-year portfolio of high-value work across information security, privacy, IT risk management, asset management and infrastructure, advising some of the world’s most respected organizations across the United States, Latin America and Europe. He examined the measurable value of technology capability in risk mitigation in his 2011 book *Webify*, and has served on the board of a public investment trust and on the senior executive committee of a \$5B Nasdaq company.

Andrew Patterson, Chief Operating Officer. Andrew Patterson leads the delivery and optimization of ArxNimbus’s cyber and AI risk-management solutions, drawing on a career that bridges public service and the private sector. In government, he served as Deputy Chief of Staff and Global Risk Advisor at the U.S. Department of Energy and as liaison to the National Security Council, shaping risk-management strategy at the highest levels of decision-making. In the private sector, he worked with PwC’s Research and Insights team analyzing emerging global risks, and with leading hedge funds and commodity traders navigating complex operational and portfolio risk. Across decades of practice, he has pioneered approaches to emerging-threat analysis, cyber strategy and enterprise risk frameworks that marry the tactical with the strategic.