

2026 RESEARCH REPORT · OCTOBER 2026

The State of Vulnerability Remediation in 2026

What goes wrong at 11–50 person tech companies, and how to fix it

EXECUTIVE SUMMARY

Exploited vulnerabilities are now the top way breaches start

In 2026, exploiting a known vulnerability became the most common way breaches start, and most companies are fixing those vulnerabilities more slowly than they did a year ago. For an 11–50 person tech company, the hard part is choosing the small number of vulnerabilities that matter and closing them within days.

31%	of breaches now start with vulnerability exploitation, up from 20% a year earlier. Source: Verizon DBIR 2026
26%	of actively exploited (CISA KEV) vulnerabilities were fully remediated, down from 38%. The median time to fix a critical one rose from 32 to 43 days. Source: Verizon DBIR 2026, via Simulint
–7 days	is the estimated mean time to exploit: on average, attacks begin before the vulnerability is public. Source: Mandiant M-Trends 2026, via Security Boulevard
35,364	CVEs were published in the first half of 2026, up 49.5% on the same period of 2025. Only 0.24% have been confirmed as exploited so far. Source: Jerry Gamblin, CVE Mid-Year 2026
48%	of breaches involved a third party, up 60% year over year. Source: Verizon DBIR 2026
\$6.29M	is the average breach cost in financial services and \$5.50M in technology. Source: IBM Cost of a Data Breach 2026, via eSecurity Planet

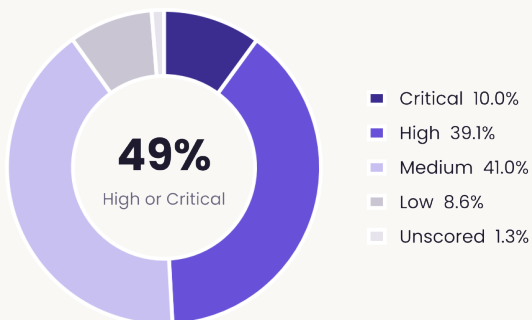
The short version: a small team can close most of this gap with a short process that is actually enforced. Know what you run, rank issues by exploitation evidence instead of CVSS alone, set deadlines in days for the few issues that matter, and automate dependency updates.

01 · THE 2026 LANDSCAPE

Every headline measure got worse

Between the 2025 and 2026 reports, more vulnerabilities were published, more breaches started with one, and fewer of the dangerous ones were closed.

Measure	2025 report	2026 report	Source
Breaches that start with vulnerability exploitation	20%	31%	Verizon DBIR
Exploited (KEV) vulnerabilities fully remediated	38%	26%	Verizon DBIR
Breaches involving a third party	30%	48%	Verizon DBIR
CVEs published, January to June	23,656	35,364	Jerry Gamblin
Open source vulnerabilities per codebase (mean)	280	581	Black Duck OSSRA
Organizations carrying security debt (flaws open over a year)	74%	82%	Veracode SoSS
Median dependency lag behind latest major version	215 days	278 days	Datadog DevSecOps
Global average cost of a breach	\$4.44M	\$4.99M	IBM, via eSecurity Planet



Half of new CVEs are rated High or Critical. Almost none are exploited.

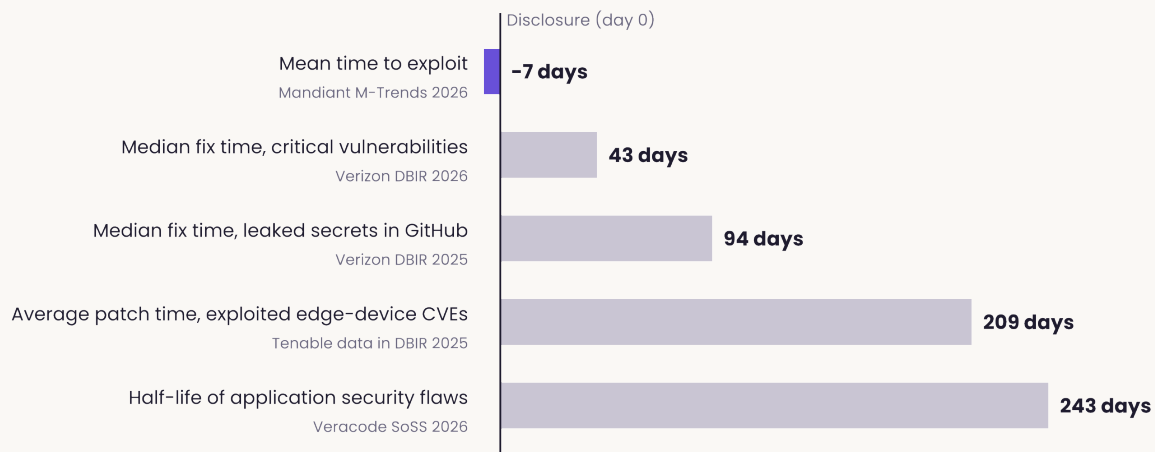
Of the 35,364 CVEs published in H1 2026, 49% carry a High or Critical CVSS rating. Only 85 of them (0.24%) have been added to the [CISA KEV catalog](#) so far.

CVE output is on track for roughly 71,000–72,000 this year, so most of the work is triage. A team that treats every High or Critical finding as urgent will spend its time on issues that attackers are not using.

Severity of CVEs published January–June 2026. Source: [Jerry Gamblin](#)

The bigger risk is the gap between attack and fix

Attackers start a week before disclosure on average. Most fixes take six weeks to eight months.



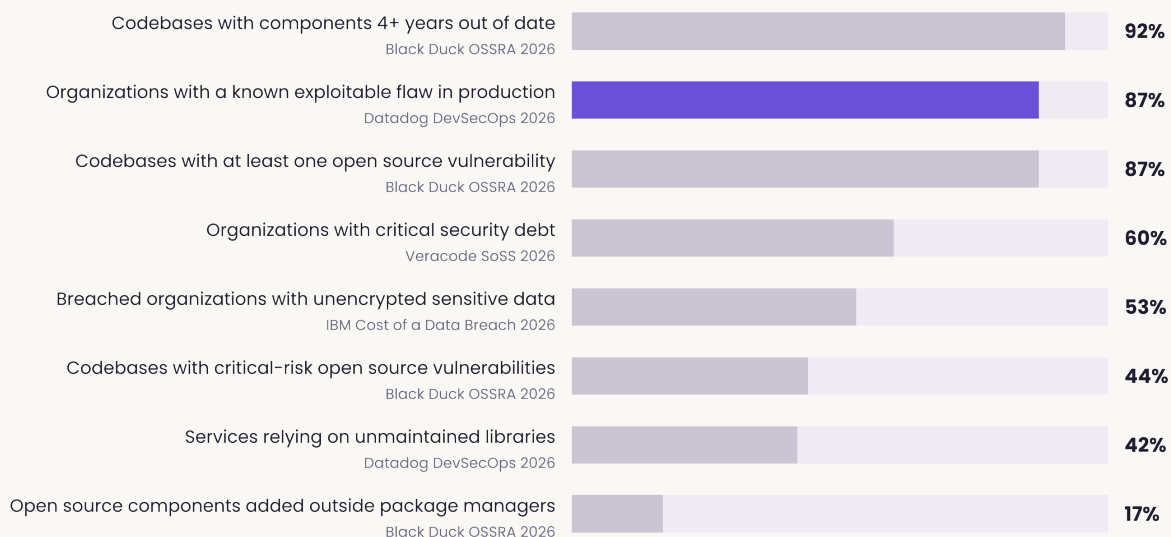
Days measured from public disclosure. Sources: [Mandiant M-Trends 2026](#), [Verizon DBIR 2026](#), [Verizon DBIR 2025](#), [Tenable](#), [Veracode SoSS 2026](#)

A 43-day median fix time sounds reasonable until it is set against exploitation that starts a week before disclosure. Verizon also found that 35% of exploited vulnerabilities were still open after 28 days, and even mature programs left 60–70% open after one week.

02 · WHAT GOES WRONG MOST OFTEN

Known, exploitable flaws are in production at 87% of organizations

Most companies already know about the vulnerabilities that hurt them. The failures sit in prioritization, dependency upkeep and ownership, and they are close to universal.



Share of organizations, codebases or components affected. Sources: [Black Duck OSSRA 2026](#), [Datadog 2026](#), [Veracode SoSS 2026](#), [IBM 2026](#)

Seven failure patterns account for most of the gap

Each one is sharper at 11–50 people, where security is usually a part-time job for an engineer or the CTO.

Failure pattern	What the data shows	How it shows up at 11–50 people
Ranking by CVSS alone	49% of HI 2026 CVEs were rated High or Critical; 0.24% are confirmed exploited (Gamblin). Veracode puts real-world danger at 11.3% of flaws (IT Brief).	The scanner shows hundreds of “criticals.” The team either ignores the list or spends a sprint on the wrong items.
Stale dependencies and end-of-life runtimes	Services on end-of-life runtimes carry exploitable flaws 50% of the time vs. 31% on supported versions. Services deployed less than monthly run dependencies 295 days behind vs. 172 for daily deployers (Datadog).	Major upgrades get deferred because they break things, so the backlog compounds.
Incomplete inventory	17% of open source components arrive outside package managers (OSSRA). Only 59% of new CVEs carry the product data needed for automatic matching (Gamblin).	No one can answer “are we affected?” within an hour of a big disclosure.
Internet-facing and remote-access devices	Edge devices and VPNs grew from 3% to 22% of exploitation targets; only 54% of exploited edge CVEs were fully patched (CSO Online , ITWire).	A forgotten VPN, admin panel or staging box stays exposed for months.
Third parties and SaaS vendors	48% of breaches involve a third party (Verizon). 66% of critical security debt sits in third-party code (IT Brief).	Vendor access and integrations are added fast and rarely reviewed.
The old backlog	80% of persistently exploited KEV entries were registered before 2024 (Simulint). CISA added 94 pre-2025 CVEs to KEV in 2025 (Brandefense).	Last year’s “accepted risk” items are never revisited.
AI tooling treated as internal	Two AI developer tools (Marimo, LiteLLM) entered KEV in HI 2026 (Brandefense). 92% of organizations with AI-related incidents lacked proper AI access controls (IBM).	LLM proxies, notebooks and agent frameworks hold API keys but sit outside scanning.

Behind all seven is capacity. Veracode found teams fix about 10% of open flaws each month ([I Programmer](#)), and IBM found only 18% of organizations use AI agents for vulnerability management ([eSecurity Planet](#)).

03 · HOW TO FIX IT

Fix a short list fast. Schedule the rest.

A small company can close most of this gap without a security team. Fewer than 1% of new CVEs are confirmed exploited ([Gamblin](#)), and teams that deploy daily keep dependencies about 40% fresher than teams that deploy monthly ([Datadog](#)).

The process we recommend looks like this. If you want help running steps 1 to 3, see our [vulnerability scanning service](#).

- 1 Build one inventory.** List every repository, cloud account, internet-facing host, SaaS vendor with access to your data, and AI tool holding API keys. Generate an SBOM for each production service so “are we affected?” takes minutes.
- 2 Rank by exploitation, then exposure.** Start with anything in the [CISA KEV catalog](#), then a high EPSS score, then whether the system is internet-facing or holds customer data. Use CVSS to break ties, not to set the order.
- 3 Set deadlines in days and track them.** Use the tiers in the table below. Measure each finding from the day it is detected, not the day someone opens the ticket.
- 4 Automate dependency updates.** Turn on Dependabot or Renovate, group minor and patch updates, and merge them weekly. Schedule one major-version upgrade per quarter and retire end-of-life runtimes first.
- 5 Shrink what is reachable from the internet.** Remove unused admin panels, staging hosts and VPNs. Put the rest behind SSO and MFA, including vendor and contractor access.
- 6 Scan for secrets and rotate them.** Run secret scanning on every push and rotate any exposed key the same day.
- 7 Give it one owner and three numbers.** Name an engineer as owner and review monthly: share of KEV findings closed within deadline, median days to fix criticals, and count of findings older than 90 days.
- 8 Reuse the work for compliance.** SOC 2 (CC7.1) and ISO 27001 (Annex A 8.8) both expect a defined vulnerability process with remediation timelines and evidence. The same tickets and reports become audit evidence.

Tier	What qualifies	Recommended deadline
P0	In CISA KEV or has a public exploit, on an internet-facing system or one holding customer data	Mitigate in 24 hours, fix in 72 hours
P1	In KEV or high EPSS on internal systems; Critical CVSS on internet-facing systems	7 days
P2	High severity and reachable in production	30 days
P3	Everything else	90 days, reviewed quarterly

These deadlines are a starting point for an 11–50 person team, not a standard. For reference, US federal agencies must fix KEV entries within two weeks under CISA BOD 22–01, and the DBIR median for critical fixes is 43 days. A team that hits P0 and P1 consistently will be well ahead of both.

04 · A 90-DAY PLAN

A working program in one quarter

Most 11–50 person companies can get there with a few hours of engineering time a week.

Days 1–30	Days 31–60	Days 61–90
Build the inventory, turn on dependency and secret scanning, list every internet-facing asset, and close any open KEV findings.	Adopt the P0–P3 deadlines, name an owner, set up automated dependency updates, and remove or lock down unused external access.	Report the three monthly numbers, work down findings older than 90 days, plan the first end-of-life runtime upgrade, and file the evidence for SOC 2 or ISO 27001.

How cloudsapio helps

cloudsapio works with tech companies to set up vulnerability management that holds up in a SOC 2, ISO 27001 or HIPAA audit. We map your assets, set deadlines that fit your team, configure the tooling, and produce the evidence auditors ask for. See how our [vulnerability scanning service](#) works, or to see where you stand today, book a free 45-minute gap analysis at cloudsap.io/gap-analysis.

Sources: [Verizon 2026 DBIR, SMB infographic](#) · [Simulint, summary of 2026 DBIR vulnerability findings](#) · [Jerry Gamblin, CVE Mid-Year 2026 Check-In](#) · [Black Duck, 2026 OSSRA report](#) · [Veracode, 2026 State of Software Security](#) · [Datadog, State of DevSecOps 2026](#) · [eSecurity Planet, IBM 2026 Cost of a Data Breach key findings](#) · [Brandefense, Vulnerability Exploitation Trends H1 2026](#) · [Security Boulevard, Mandiant M-Trends 2026 time to exploit](#) · [CSO Online, DBIR 2025 edge devices and remediation](#) · [ITWire, Tenable research in Verizon DBIR](#) · [IT Brief, Veracode security debt findings](#) · [Security Magazine, DBIR 2025 leaked secrets remediation](#) · [I Programmer, Veracode SoSS 2026 summary](#)