SECURITY BASECAMP

WHITEPAPER · OCTOBER 2026

The AI Vulnerability Surge

What record CVE volumes in 2026 mean for RIAs, financial advisors and financial institutions, and the strategic and tactical actions to take now

Paul Osterberg
Managing Director & CEO, Security Basecamp LLC

Data current as of October 27, 2026. This paper is for informational purposes and is not legal advice.

Executive summary

AI-driven vulnerability discovery has roughly tripled the rate at which software flaws are published in 2026. For financial firms, patching capacity, not awareness, is now the constraint.

3.6x
Microsoft CVEs in 2026 vs. all of 2025

1.8x
Industry-wide CVEs in 2026 vs. all of 2025

1,413
Microsoft CVEs in October alone, more than any prior full year

- **Microsoft:** About 4,090 Patch Tuesday CVEs through October 2026, versus 1,130 in all of 2025 (about 3.6x). October alone (1,413) exceeded any prior full year.
- **Industry-wide:** 86,533 CVEs published through October 25, 2026, versus 48,185 in all of 2025 (about 1.8x). Q3 2026 ran about 3.2x Q3 2025.
- **Timing:** The surge follows Anthropic's April 7, 2026 launch of Project Glasswing, which gave Microsoft and other vendors access to the Claude Mythos Preview model for defensive bug-hunting. Other AI tools are contributing too.
- **What has not changed:** Only a small fraction of CVEs are ever exploited. The share is falling, not rising.

The implication for RIAs, broker-dealers, advisors and other financial institutions is that "patch everything quickly" no longer scales. Firms need exploitation-based prioritization, a smaller attack surface, tighter oversight of the MSPs and vendors who do their patching, and resilience for the day a fix arrives too late. Regulators (SEC Reg S-P, FINRA, NYDFS Part 500) already expect each of these.

What changed in 2026

Frontier AI models can now find exploitable bugs in mature code at a pace human researchers never could. Software vendors are publishing the results.

- **April 7, 2026:** Anthropic launched Project Glasswing, giving a small group of partners, including Microsoft, Amazon, Apple, Google, CrowdStrike and the Linux Foundation, early access to Claude Mythos Preview for defensive vulnerability research.
- **April 22, 2026:** Microsoft confirmed its participation. It later said it would build Mythos Preview into its Security Development Lifecycle.
- **April 2026:** According to internal Microsoft material reported by ProPublica, Mythos surfaced 90 critical and 141 important vulnerabilities in SharePoint alone in a single month.
- **July 2026:** Microsoft warned customers to expect a sustained surge in security updates driven by its use of AI to find vulnerabilities.

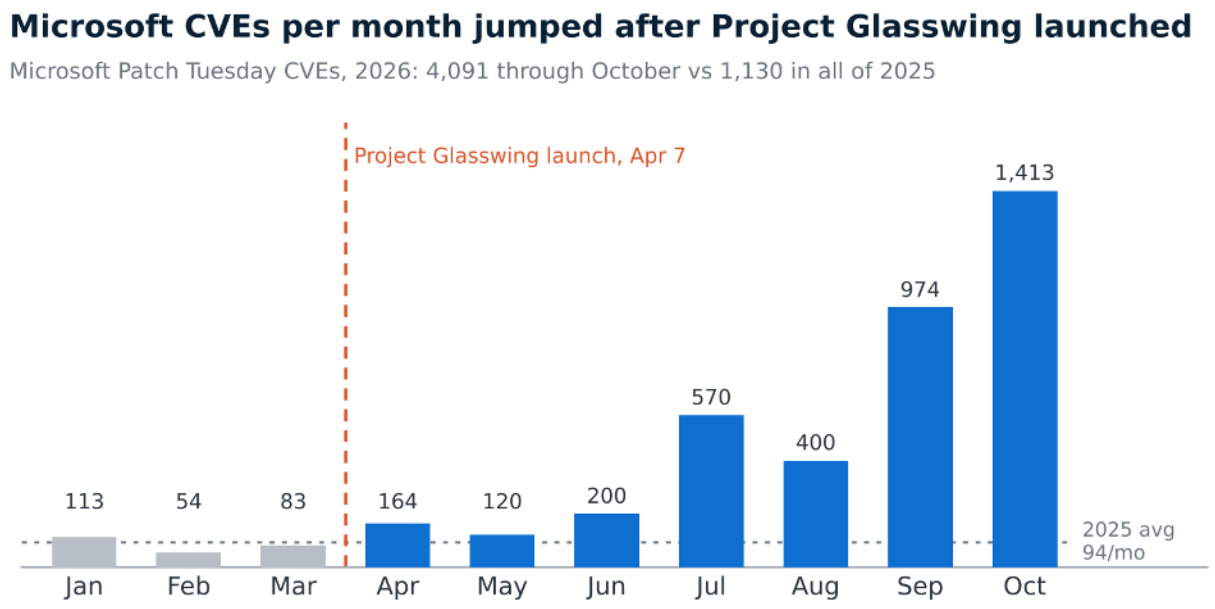
© 2026 Security Basecamp LLC · securitybasecamp.com · entrustiq.io

THE KEY POINT

These are mostly long-standing flaws, some decades old, that are now being found faster. They are not new bugs. The defects were always in the software you run. What changed is that they are now being found and published, and attackers with similar AI tools can find the same ones.

The data: Microsoft

Microsoft has published roughly 4,090 Patch Tuesday CVEs in 2026, more than three times its previous record year.



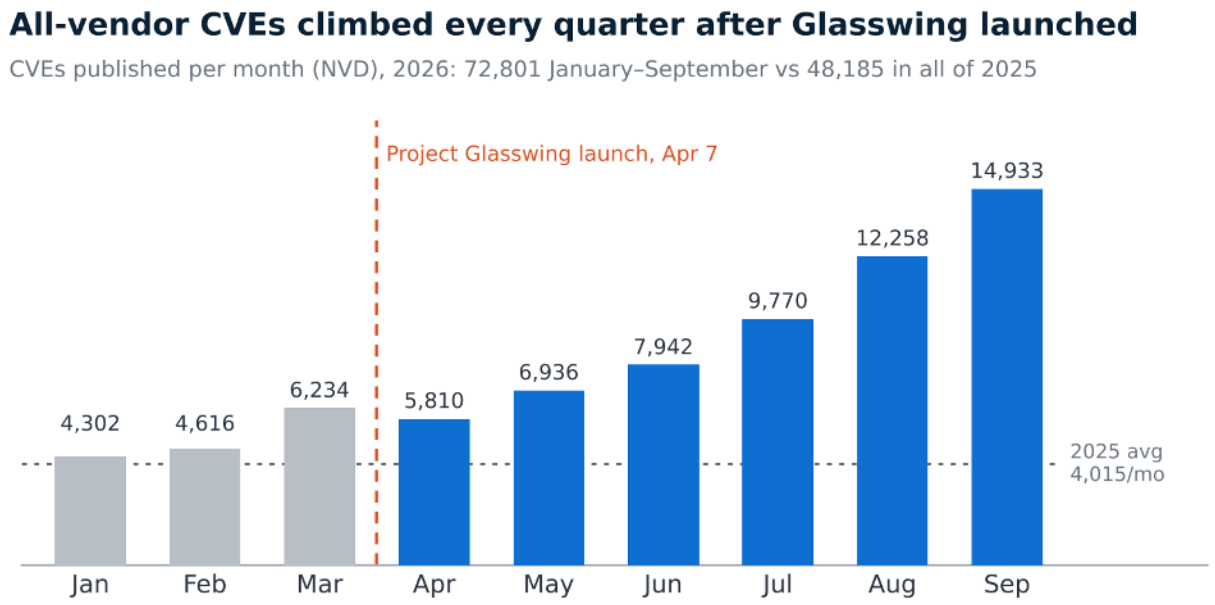
Sources: Infosecurity Magazine, Security Affairs (ZDI), Tenable. Microsoft Patch Tuesday CVEs, January to October 2026.

January through March were in line with history, at about 250 CVEs combined. Every month from June onward set a new record, and October became the first four-digit release. Since April, the monthly average has been about 550, roughly six times the 2025 pace.

Year	Microsoft Patch Tuesday CVEs	Multiple of 2025
2020 (prior record)	1,245	1.1x
2024	1,009	0.9x
2025	1,130	1.0x
2026 (through October)	~4,090	~3.6x

The data: all vendors

Industry-wide, 86,533 CVEs were published through October 25, 2026, about 1.8 times all of 2025 with two months still to go.



Sources: NVD via Brandefense (by published date, rejected records excluded); 2025 total from Jerry Gamblin's 2025 CVE Data Review.

The industry curve rose more gradually than Microsoft's, but by September monthly volume was about 3.7 times the 2025 average. Q3 2026 alone ran about 3.2 times Q3 2025. The most severe flaws rose fastest: among 21 major organizations tracked by Epoch AI, high- and critical-severity CVEs reached about 1,500 in June (3.5 times the pre-Mythos monthly record) and about 2,500 in July (about 5 times). FIRST's raised forecast of about 66,000 CVEs for all of 2026 was already exceeded by September.

Measure	Microsoft	All vendors (NVD)
2026 year to date vs. full-year 2025	~3.6x	~1.8x
Recent run rate vs. 2025	~6x (Apr–Oct monthly average)	~3.2x (Q3 vs. Q3)

Microsoft's multiple is higher because it is a Glasswing partner fixing its own code. The industry total is diluted by a large baseline of CVEs unrelated to AI, such as WordPress plugin flaws. For context, industry-wide annual totals were about 19,200 in 2020, 40,009 in 2024 and 48,185 in 2025.

Reading the numbers correctly

The volume is real, but the risk has not risen in proportion. Five caveats keep the message accurate.

- **Attribution is circumstantial.** The surge coincides with Glasswing, but published data cannot prove which flaws AI found. Other AI programs, including OpenAI's, and vendors' own tools also contribute.
- **Counts vary by source.** Microsoft's own October figures range from 1,411 to 1,414 depending on which list is used. Industry trackers differ by hundreds to thousands. Cite one source consistently.
- **Headline counts understate Microsoft's total.** In September, Microsoft fixed about 204 cloud vulnerabilities (Azure, Entra ID, Edge) outside the Patch Tuesday headline count.
- **Severity scoring has collapsed.** NIST's enrichment rate fell from 87.1% in 2025 to 8.4% in Q3 2026. Most new CVEs carry no NIST severity score, so firms must rely on vendor ratings and exploitation data.
- **Exploitation is rare and getting rarer.** Through July 2026, only 3.77 of every 1,000 published CVEs entered CISA's Known Exploited Vulnerabilities (KEV) catalog, down from 5.54 in 2025. Most months, Microsoft flags only one or two CVEs as actively exploited.

Why it matters for financial services firms

Most RIAs and smaller financial institutions do not patch their own systems. An MSP, a custodian or a SaaS vendor does, so this surge lands on a supply chain the firm must oversee but does not control.

- **Patch workload has outgrown manual processes.** A firm that reviewed about 100 Microsoft CVEs a month in 2025 now faces 400 to 1,400.
- **The window to exploitation is shrinking.** Attackers have access to similar AI tools. Once a fix is published, it can be reverse-engineered quickly into a working attack.
- **Concentration risk is higher.** Custodian portals, CRM, portfolio management, e-signature and Microsoft 365 hold client NPI. A flaw in any one of them exposes every firm that uses it.
- **End-of-support deadlines are arriving at the same time.** Microsoft's October 2026 release was the last for several products, including Windows 11 24H2 Home/Pro and Exchange Server 2016/2019 Extended Security Updates. Systems that keep running after support ends will accumulate unpatched flaws at the new, higher rate.

The regulatory lens

Regulation	What it expects that this surge tests
SEC Reg S-P (amended)	Written incident response program; service-provider oversight, including notice to the firm within 72 hours of a breach; customer notification within 30 days. Now in force for both large and small entities.

Regulation	What it expects that this surge tests
SEC Reg S-ID	Identity theft red-flag program for covered accounts; credential compromise via an unpatched flaw is a red-flag scenario.
FINRA Rules 3110 and 4370	Reasonably designed supervision of technology and vendors; business continuity plans that survive a vendor or platform outage.
NYDFS 23 NYCRR Part 500	Risk-based vulnerability management with timely remediation (500.5), complete asset inventory (500.13), third-party service provider policy (500.11), 72-hour notification (500.17), board reporting (500.4).

WHAT EXAMINERS WILL LOOK FOR

Examiners will not expect firms to patch 1,400 CVEs a month. They will expect a documented, risk-based method for deciding which ones matter, and evidence that the firm and its vendors followed it.

Strategic actions

Seven shifts, owned by leadership and the CCO/CISO, position the firm for sustained high vulnerability volume rather than a one-time spike.

1. **Reset governance and risk appetite.** Brief principals or the board on the 2026 data. Update the written risk assessment to treat AI-accelerated discovery as a standing condition. Approve a vulnerability management policy with explicit remediation timelines.
2. **Prioritize by exploitation, not volume.** Rank fixes by known exploitation (CISA KEV, vendor "Exploitation Detected" flags), likelihood of exploitation (EPSS, vendor "Exploitation More Likely" ratings), internet exposure, and whether the system holds client NPI. Adopt tiered service levels such as the baseline below.
3. **Shrink the attack surface.** Maintain a complete asset inventory. Retire end-of-support software. Remove or gate internet-facing services, such as by putting remote access behind a VPN or zero-trust broker. Consolidate overlapping applications. Every product retired is a patch stream eliminated.
4. **Make vendors and MSPs carry measurable obligations.** Write patch timelines, monthly patch-compliance reporting, KEV response times, and Reg S-P 72-hour breach notice into contracts. Re-tier critical vendors such as custodians, CRM and portfolio platforms based on the client data they hold.
5. **Plan for the patch that arrives too late.** Strengthen compensating controls: phishing-resistant MFA, EDR/MDR with 24x7 response, least privilege, immutable backups, and network segmentation. Exercise the incident response plan against a scenario where a flaw is exploited before a fix exists.
6. **Use AI defensively, with governance.** Ask security vendors and MSPs how they use AI to triage and patch. Pilot AI-assisted tools for vulnerability triage and log review under the firm's AI acceptable-use policy.

© 2026 Security Basecamp LLC · securitybasecamp.com · entrustiq.io

7. **Fund capacity, not just tools.** Budget for patch automation, managed detection and response, and additional MSP hours. Expect 2027 security operations costs to rise.

Suggested remediation tiers

Tier	Criteria	Suggested target
1	Known exploited (KEV or vendor-flagged) on an internet-facing system or one holding client NPI	72 hours, or mitigate immediately
2	Known exploited, internal system	7 days
3	Critical severity, internet-facing	7 days
4	Critical internal, or High with "Exploitation More Likely"	14 to 30 days
5	All other	Next normal patch cycle, up to 60 days

These targets are a suggested starting point; firms should calibrate them to their own risk assessment and document the rationale. For reference, CISA's directive for federal agencies sets two weeks for KEV items.

Tactical actions: the next 90 days

Most of these steps can be done with existing staff and the firm's MSP. The first ones close today's exposure; the later ones put a repeatable process in place.

First 30 days: close current exposure

- ☐ Confirm the October 2026 Microsoft updates are installed and machines restarted on every endpoint and server, starting with the actively exploited Windows Shell flaw (CVE-2026-96951)
- ☐ Confirm automatic updates are on for Windows, Microsoft 365 Apps, browsers and PDF readers, and enforce restarts within a set window
- ☐ Identify every end-of-support system, especially on-premises Exchange 2016/2019 and Windows editions whose support ended in October 2026, and set a retirement or isolation date for each
- ☐ Run an external scan of internet-facing assets: remote access, VPN, firewalls, email gateways, and the website
- ☐ Verify phishing-resistant MFA on email, custodian portals, remote access and all admin accounts
- ☐ Subscribe the firm and its MSP to CISA KEV alerts and Microsoft security update notifications

Days 31 to 60: put the process in place

- ☐ Adopt the tiered remediation policy and add it to the written information security program
- ☐ Require monthly patch-compliance reports from the MSP: percentage of devices current, the oldest missing critical patch, and KEV items open
- ☐ Send the vendor questionnaire (next section) to critical vendors and record the answers in the vendor risk file

- ☐ Test a restore from immutable or offline backup and record how long it took
- ☐ Update the incident response plan with the Reg S-P 30-day customer notice and 72-hour service-provider notice workflows, and NYDFS 72-hour notice where applicable

Days 61 to 90: test and report

- ☐ Run a tabletop exercise: a critical flaw in a key vendor platform is exploited before a patch exists
- ☐ Update the annual risk assessment to reflect AI-accelerated vulnerability discovery
- ☐ Report patch metrics, vendor results and residual risks to principals or the board
- ☐ Set a 2027 budget line for patch automation, MDR and MSP capacity

Questions to ask your vendors and MSP

These questions turn the vendor oversight expectations in Reg S-P and Part 500 into evidence an examiner can review. Responses should be in writing.

Area	Question
Volume	How has your patch volume changed in 2026, and have you added staff or automation to keep pace?
Prioritization	How do you decide what to patch first? Do you track CISA KEV and vendor exploitation flags?
Timelines	What are your contractual remediation targets for actively exploited and critical vulnerabilities?
Evidence	Can you provide monthly patch-compliance metrics for our environment, including open KEV items and the oldest missing critical patch?
End of support	Which systems in our environment, or in your platform, run software that is past or near end of support?
Notification	Will you notify us within 72 hours of a breach affecting our clients' information, as Reg S-P requires? Who is the contact?
AI	Do you use AI to find or triage vulnerabilities in your own product? Are you a Glasswing or similar program participant?
Resilience	If a critical flaw in your platform is exploited before a fix exists, what compensating controls and communication do you provide?

Conclusion

The 2026 vulnerability surge is a lasting change, not a spike. AI has made finding bugs cheap, and vendors will keep publishing at this pace. The firms that come through it well will be the ones that know what they run, patch what is actually being exploited first, hold their vendors to measurable commitments, and can recover when a fix comes too late.

© 2026 Security Basecamp LLC · securitybasecamp.com · entrustiq.io

SECURITY BASECAMP powered by EntrustIQ

Security Basecamp is a cybersecurity consulting firm serving regulated financial services firms. We deliver cybersecurity risk assessments, vCISO advisory, third-party vendor risk due diligence, cloud security assessments and penetration testing. EntrustIQ, our risk and compliance platform, turns that work into a repeatable, exam-ready program.

Paul Osterberg · POsterberg@securitybasecamp.com · securitybasecamp.com · entrustiq.io

Sources

All figures as of October 27, 2026. Counts vary by tracker.

1. Infosecurity Magazine: Microsoft September 2026 record and monthly counts
2. Security Affairs: October 2026 Patch Tuesday (ZDI count)
3. Splashtop: October 2026 Patch Tuesday breakdown
4. IT-Connect: October 2026 end-of-support editions
5. Tenable: Microsoft Patch Tuesday 2025 Year in Review
6. Tenable: March 2026 Patch Tuesday review
7. BetaNews: Mythos and Microsoft (ProPublica reporting)
8. PYMNTS: Microsoft joins Project Glasswing
9. Brandefense: CVE Statistics 2026 (NVD monthly counts)
10. Jerry Gamblin: 2025 CVE Data Review
11. Cyber Strategy Institute: NVD enrichment rate
12. Axis Intelligence: KEV signal density
13. Epoch AI: High and critical CVE spike
14. WinBuzzer: Limits of the attribution data
15. Help Net Security: FIRST 2026 forecast