



BEYOND VULNERABILITY SEVERITY:

EXPLORING HOW EXPOSURES COMBINE
TO AMPLIFY CYBER RISK

SEPTEMBER, 2026

OUTLINE

Executive Summary.....	03
Methodology.....	04
Global Threat Landscape.....	05
The “Low Severity” Problem.....	10
What Attackers Prioritise.....	16
Recommendations.....	20

Executive Summary

Most organisations have more security vulnerabilities than they can realistically address, making effective prioritisation important. However, severity scores may not always reflect which vulnerabilities are most likely to be exploited. The evidence examined in this report suggests that only a small proportion of vulnerabilities recorded in the U.S. National Vulnerability Database have been confirmed as exploited, while medium-severity vulnerabilities can still feature significantly in observed exploitation activity.

The report also examines how attackers may combine vulnerabilities with identity and credential weaknesses, misconfigurations, excessive permissions, exposed services and access-control gaps to amplify attack paths. Evidence from more data and selected 2026 case studies illustrates how different weaknesses and access points can contribute to an attack.

The report concludes by examining approaches that look beyond individual vulnerability scores to consider how weaknesses connect to critical assets. This includes exposure management, attack-path analysis and Continuous Threat Exposure Management (CTEM), which place greater emphasis on understanding and addressing exposures in their broader context.



31%

of all breaches start with
vulnerability exploitation

[12]



Methodology

Data Collection & Source Selection

The data used in this report were deliberately selected to examine how vulnerabilities and other security exposures contribute to cyber risk, with particular emphasis on the relationship between severity, exploitability, exposure, attacker behaviour, and attack paths. The collection process focused on obtaining verifiable evidence capable of illustrating:

- how technical severity differs from observed exploitation and practical attacker behaviour
- how attackers combine vulnerabilities with credentials, misconfigurations, excessive privileges, and exposed services to develop attack paths
- how accessibility, reliability, privilege gained, and proximity to critical assets influence attacker prioritisation
- how seemingly low- or medium-severity weaknesses can contribute to broader compromise when combined with other exposures.

To ensure relevance and credibility, sources were drawn from three primary categories:

1. Vulnerability and Exploitability Databases: Structured vulnerability datasets and exploitation indicators were analysed to examine vulnerability severity, volume, and evidence of exploitation. These included NVD/CVSS, EPSS, and the CISA Known Exploited Vulnerabilities (KEV) catalogue.

2. Threat Intelligence and Attack-Path Research: Authoritative threat intelligence reports, MITRE ATT&CK, and attack-path research were used to examine attacker behaviour, exploitation techniques, identity and credential weaknesses, misconfigurations, privilege escalation, lateral movement, and access to critical assets.

3. Documented Incidents and Case Studies: Real-world breach reports and incident analyses were reviewed to illustrate how different weaknesses, including social engineering, identity and access issues, and trusted third-party relationships, can form part of broader attack paths.

Data Selection Criteria

All datasets and sources were selected based on the following criteria:

Verifiability: Sourced from reputable cybersecurity organisations, government agencies, recognised research institutions, vulnerability databases, or documented incidents.

Recency: Prioritising recent evidence, particularly 2025–2026 data, to reflect current exploitation and attacker behaviour.

Relevance: Focusing on evidence directly related to vulnerability severity, exploitability, exposure, attacker prioritisation, and attack paths.

Analytical Value: Ensuring the data could support comparisons between severity and exploitation, identify relationships between different exposures, and demonstrate how individual weaknesses can contribute to broader attack paths.

GLOBAL THREAT LANDSCAPE

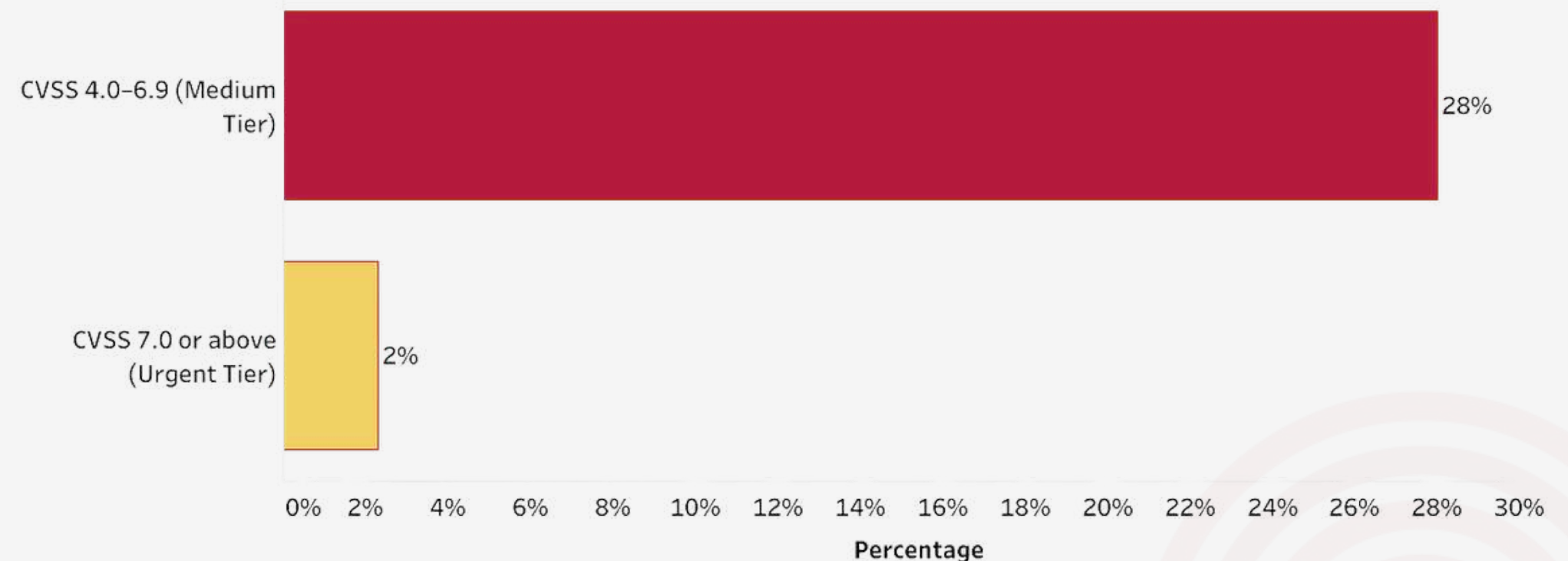
THE SEVERITY-EXPLOITABILITY GAP

Technical severity, as expressed by the Common Vulnerability Scoring System (CVSS), measures what a vulnerability could do to a system in isolation, the privileges it could grant, the damage it could cause, and how easy it is to trigger under ideal conditions. It does not explicitly measure whether attackers are actually using it, or ever will. [1]

CVSS uses a **0.0–10.0** scale, divided into five severity levels: **None (0.0)**, **Low (0.1–3.9)**, **Medium (4.0–6.9)**, **High (7.0–8.9)**, and **Critical (9.0–10.0)**. Low-severity vulnerabilities generally have limited impact or more demanding exploitation conditions, while Medium vulnerabilities may have greater but more bounded effects. High-severity vulnerabilities can enable significant outcomes such as privilege escalation, unauthorised access or data exposure, while Critical vulnerabilities represent the highest level of technical severity and may enable extensive system compromise, including some forms of unauthenticated remote code execution. CVSS therefore provides an important measure of technical severity, but it is not, on its own, a complete measure of real-world exploitability or organisational risk. Data show that:

- Only an estimated 2%–7% of all published CVEs are ever observed being exploited in the wild, according to research cited by the Forum of Incident Response and Security Teams and echoed across multiple independent studies.
- Research firm Root Evidence's Q1 2026 analysis put the figure even lower: just 1.4% of vulnerabilities in its dataset were tied to confirmed real-world exploitation, and it found a weak correlation between CVSS, exploit proof-of-concept availability, Metasploit modules and actual attacker behaviour. [13]
- Of all CVEs scoring CVSS 7.0 or above (the threshold most organisations treat as “urgent”), FIRST’s own research found only 2.3% were observed in exploitation attempts in a given month, per analysis from Picus Security and Brandefense.
- Conversely, medium-severity vulnerabilities (CVSS 4.0–6.9) made up 28% of all vulnerabilities actually exploited in Q1 2025, flaws that a CVSS-first remediation queue would systematically deprioritise. [5]

The gap between what CVSS calls urgent and what attackers actually use



Only 2.3% of “urgent” CVSS 7+ CVEs saw exploitation attempts in a given month, while medium-severity CVEs made up 28% of vulnerabilities actually exploited in Q1 2025. [4,5]

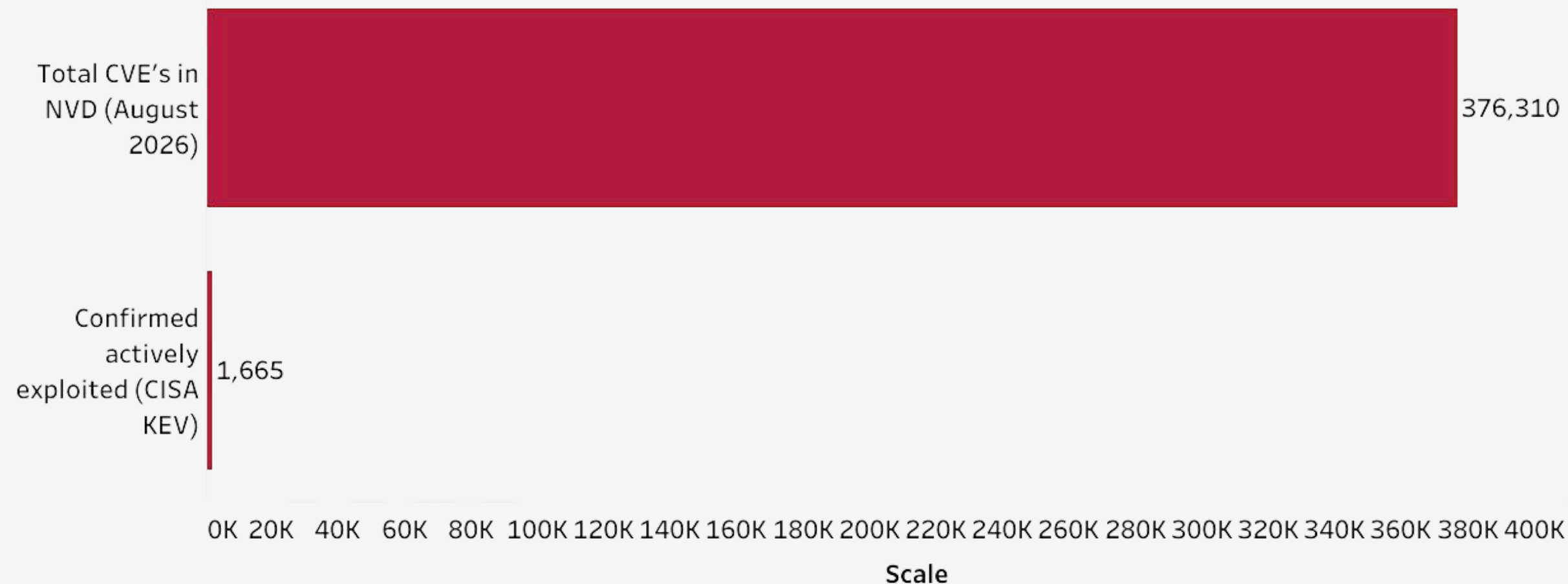
GLOBAL THREAT LANDSCAPE

Severity scoring remains a useful way to assess a vulnerability's potential technical impact, but it may not provide a complete basis for prioritisation. CVSS, for example, does not account for factors such as whether a vulnerability is internet-facing, whether compensating controls are in place, whether an exploit is available, or how closely it is connected to a valuable asset. Tools such as the Exploit Prediction Scoring System (EPSS) and the CISA Known Exploited Vulnerabilities (KEV) catalogue provide additional context by considering the likelihood or evidence of real-world exploitation alongside technical severity. [31,3]

The scale problem underneath it

Even a strong exploitability signal does not, on its own, address the broader challenge of limited remediation resources. As of August 2026, the CISA Known Exploited Vulnerabilities (KEV) catalogue contained 1,665 entries, compared with 376,310 CVE records in the NIST National Vulnerability Database. [2,3] While the KEV catalogue continues to expand, with entries increasing by 16.8% year-over-year, the comparison highlights the scale of the vulnerability population organisations may need to assess. This makes it increasingly important to identify and prioritise exposures based on evidence of exploitation, context and potential relevance to critical assets rather than treating all recorded vulnerabilities as equally actionable.

Confirmed active exploitation is a tiny, identifiable fraction of total recorded vulnerabilities



Only 0.44% of recorded CVEs are known to be exploited, yet teams still have to work through the full 376,000+. [3,6]

GLOBAL THREAT LANDSCAPE

HOW ATTACKERS BUILD ATTACK PATHS

Attackers rarely succeed by exploiting one weakness in isolation. A more common pattern is a sequence in which an initial foothold (regardless of the severity of the vulnerability that enabled it) provides access that can be expanded through credentials, privileges, misconfigurations, exposed services or other weaknesses until the attacker reaches a valuable system or asset. **The MITRE ATT&CK Enterprise Framework** provides a useful way to describe this progression. Its tactics represent the adversary's objectives, while its techniques describe how those objectives are achieved. Relevant stages include **Initial Access, Credential Access, Privilege Escalation, Discovery and Lateral Movement**, followed by activities such as Collection, Exfiltration or Impact. [7]

From Initial Access to the Target

The attack path can therefore be viewed as a sequence rather than a collection of unrelated vulnerabilities:

Initial Access → Credential Access → Privilege Escalation → Discovery → Lateral Movement → Critical Asset

- **Initial Access:** The attacker establishes a foothold through an entry point such as exploitation of a public-facing application, valid accounts or a trusted relationship. MITRE ATT&CK specifically identifies these as techniques that can provide initial access to an environment. [8]
- **Credential Access:** Once inside, the attacker may seek additional credentials that can provide access to other systems or accounts. MITRE identifies credential theft as a distinct tactic because compromised credentials can subsequently support further access and movement. [9]
- **Privilege Escalation:** The attacker may then seek higher-level permissions by taking advantage of vulnerabilities, misconfigurations or weaknesses in privilege controls. [10]
- **Discovery:** With greater access, the attacker can identify systems, accounts, services and other resources that may provide a route toward the intended target. [7]
- **Lateral Movement:** The attacker can use the access obtained to move between systems and accounts, potentially creating additional paths toward critical assets. [7]

Where Breaches Start Now

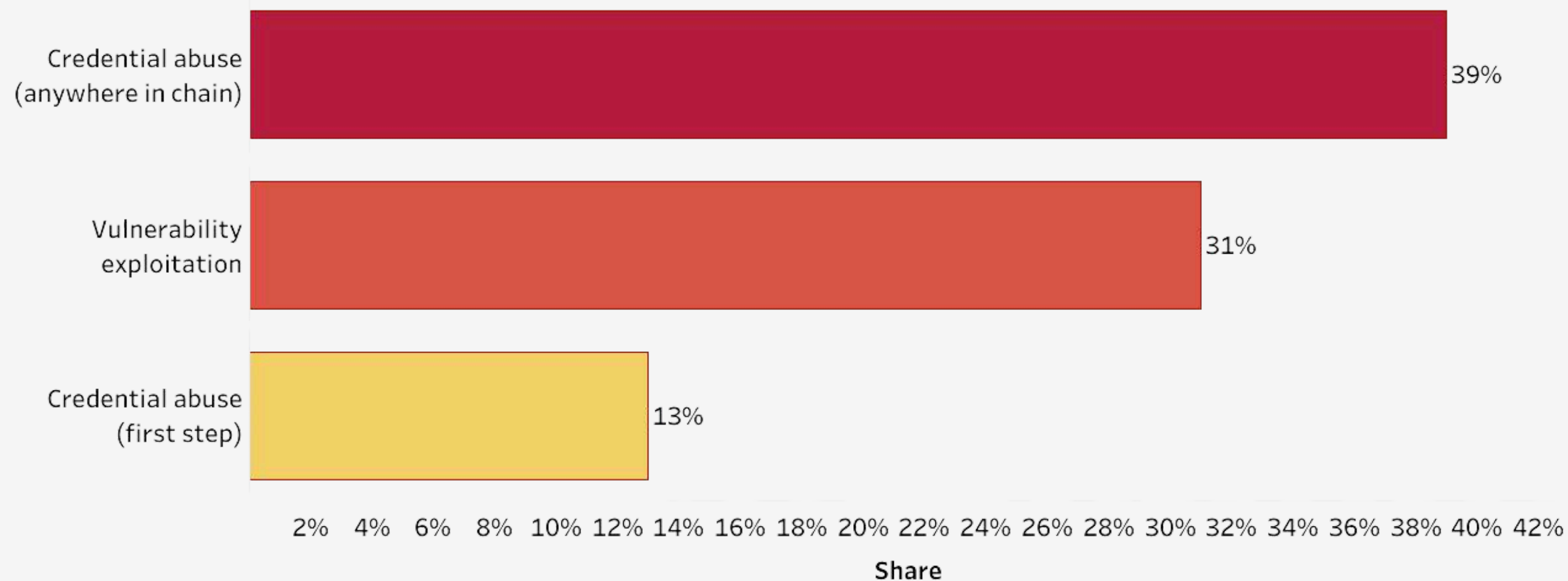
Real-world breach data provides evidence of the different ways attackers can establish that initial foothold. The 2026 Verizon Data Breach Investigations Report (DBIR), drawing on more than **22,000 confirmed breaches across 145 countries**, found that vulnerability exploitation accounted for **31% of breaches as an initial access vector**, making it the leading entry point in its dataset. Credential abuse accounted for **13%** when measured as the first identified action. Verizon also notes that this decline is partly related to the introduction of a separate pretexting category; when credential abuse is considered at any point in the breach progression, it appears in **39% of breaches**. [12]

22,000 confirmed
breaches across 145
countries
[12]

GLOBAL THREAT LANDSCAPE

This distinction is important for understanding attack paths. A credential may not be the initial entry point, but it can become important later in the sequence. Similarly, a vulnerability may provide the initial foothold without being the mechanism that ultimately allows the attacker to reach a critical asset.

Vulnerability exploitation now leads to the door; credentials still dominate what happens next



Vulnerability exploitation overtakes credentials as the top initial access vector for the first time in the DBIR's 19-year history, but credential abuse still surfaces somewhere in 39% of full breach chains. [12]

This is explicit: the shift is about where attackers break in, not what they reach for once they are inside. Identity remains the connective tissue of most attack paths even as the entry point has moved to the network edge.

GLOBAL THREAT LANDSCAPE

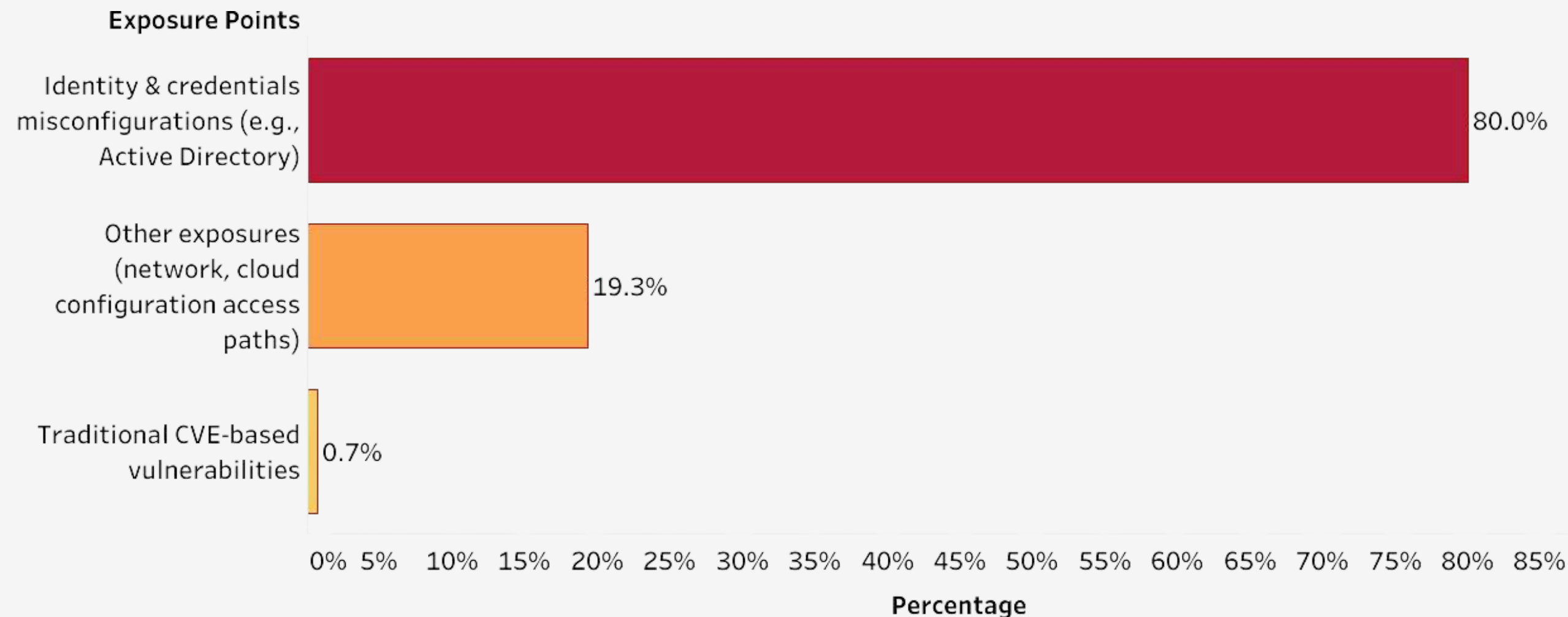
What attack paths are actually made of

Independent attack-path research adds another layer by examining the exposure landscape attackers can potentially move through after gaining access. Research by XM Cyber and the Cyentia Institute, based on more than **40 million exposures**, found that identity and credential misconfigurations accounted for roughly **80% of identified security exposures**. Much of this exposure was concentrated around identity infrastructure such as Active Directory. [17]

Traditional CVE-tracked vulnerabilities therefore represent only part of the exposure landscape. XM Cyber's research found that credential- and permission-related attack techniques affect **82% of organisations studied**, while a separate study found that **73% of top attack techniques** involved mismanaged or stolen credentials.

The implication is not that software vulnerabilities are unimportant. Rather, the attack-path perspective highlights where exploitable exposure actually lives, versus where vulnerability management programmes usually look. As the graph below illustrates, exposure can extend beyond CVE-tracked vulnerabilities to include credentials, permissions, identity systems and misconfigurations that can interact to create a sequence of access. [18]

Where exploitable exposure actually lives, versus where vulnerability management programmes usually look



Across approximately 40 million analysed exposure points, CVE-tracked vulnerabilities account for less than 1% of an organisation's exploitable attack surface. [18]

THE “LOW-SEVERITY” PROBLEM



The “Low-Severity” Problem

A security weakness does not necessarily need to be classified as critical to contribute to a serious incident. Vulnerabilities and exposures that appear low or moderate when assessed individually can become more significant when they are accessible, connected to other weaknesses, or positioned along a path to valuable systems and data. In some cases, the weakness may not be a software vulnerability at all, but rather a configuration, permission or access-control issue that traditional vulnerability assessments may not capture.

The following scenarios illustrate how seemingly limited weaknesses can contribute to broader attack paths. For each example below, the vulnerability is named, and its published CVSS score is stated.

Example 1: N-able N-central (August–September 2026)

N-central is a remote monitoring and management platform. In an earlier intrusion in July 2026 via a related authentication bypass, attackers who gained administrative access used the platform’s Take Control feature to reach managed endpoints and register Cloudflare tunnels for persistence.

The relevant point here is that a Medium-severity access-control flaw was enough to form part of a chain leading to administrative access:

- CVE-2026-86206 — an access-control flaw that allowed unauthorised access to internal APIs. N-able rated it CVSS 6.9 (Medium) in its own CVE record.

Notably, CVE-2026-86207, an authentication bypass in internal-only APIs, rated CVSS 7.7 (High), was also relevant to the attack chain. Rapid7 researcher, Stephen Fewer, showed that the two flaws could be chained to allow a remote, unauthenticated attacker to create a new System Administrator account on the server. CISA added both CVEs to its Known Exploited Vulnerabilities catalogue. [22,23]

Example 2: LiteLLM (May–June 2026)

A LiteLLM proxy stores model-provider credentials and API keys and connects onward to AI infrastructure.

Here, the Medium-severity flaw provided the initial step that made a more serious vulnerability exploitable without authentication:

- CVE-2026-48710 — a “BadHost” host-header validation bypass in the Starlette framework, which LiteLLM depends on. It was rated CVSS 6.5 (Medium).

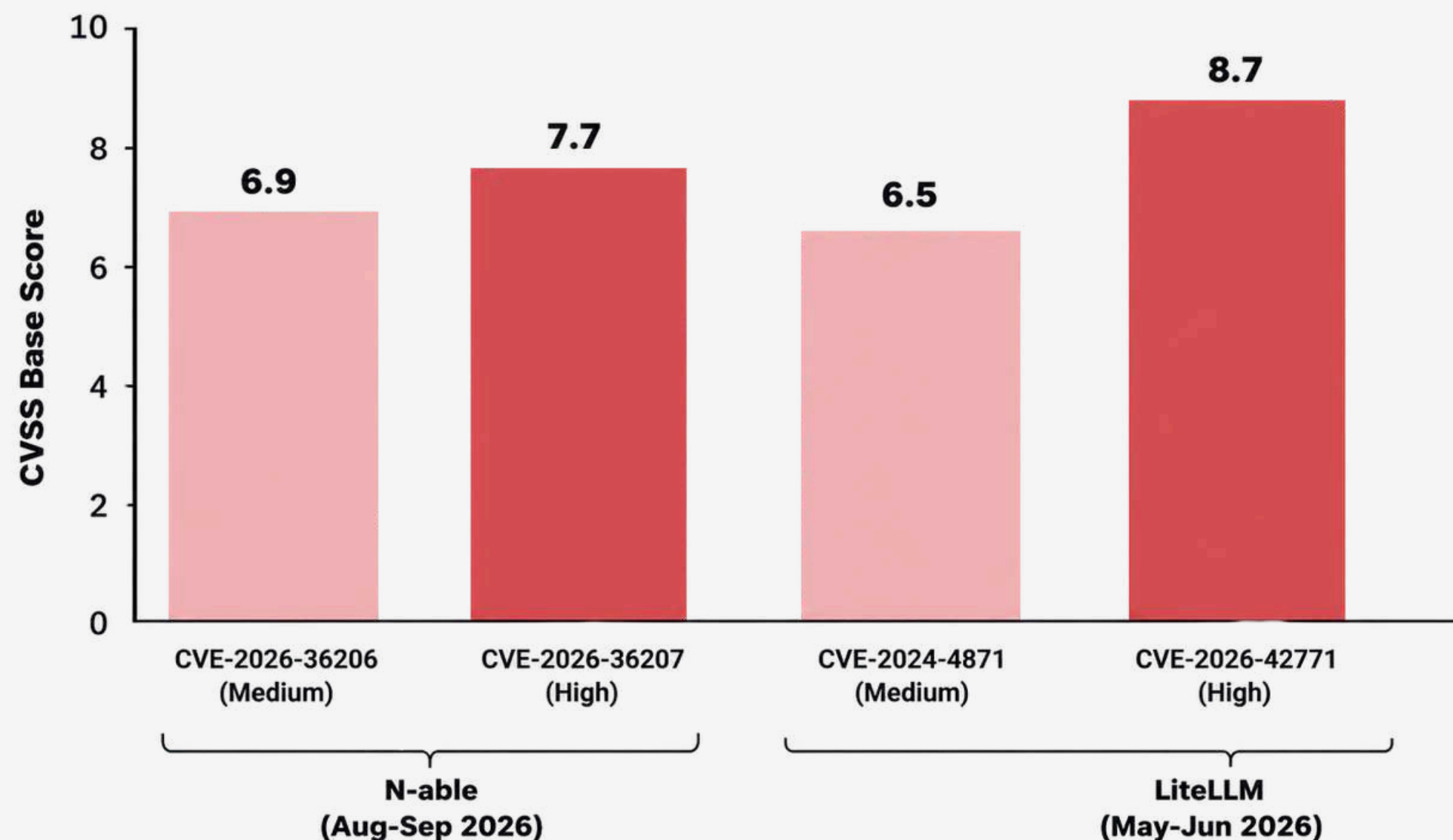
It is worth noting that CVE-2026-42271, a command-injection flaw in LiteLLM itself (was also exploited), was rated CVSS 8.7 (High). It required a valid API key on its own but became relevant to the attack chain once the authentication requirement was bypassed. CISA added it to the KEV catalogue in June 2026 following evidence of active exploitation. Horizon3.ai demonstrated that the two flaws could be chained, with the Medium-rated bypass removing the authentication requirement and enabling the High-rated command-injection flaw to achieve unauthenticated remote code execution. [24]

Under what conditions did Medium become dangerous?

- The Medium flaw removed a barrier (authentication) that the High flaw depended on, so the chain was worth more than either link.
- The affected system was reachable: an internet-exposed console or gateway.
- The system sat next to something valuable: administrative control of managed endpoints, or stored provider credentials.

The “Low-Severity” Problem

CVSS of each link in the two chains. No individual flaw is Critical



The evidence is more nuanced than “low-severity flaws are dangerous.” Both chains pair a Medium with a High. The cases show that the highest-severity link in each chain (7.7 and 8.7) fell below the Critical threshold, and the Critical outcome came from how the links connect.

The “Low-Severity” Problem

Real-World Examples of Weaknesses in Attack Paths

The three scenarios examined below illustrate how attack paths can develop through very different starting points. They include situations involving social engineering, identity and access abuse, and trusted third-party relationships, demonstrating that an attack does not necessarily depend on a conventional software vulnerability or misconfiguration. In some cases, a simple interaction can provide the initial access needed to begin a much broader compromise.

ADT (April 2026)

The available account of the breach suggests that the incident was not primarily a software vulnerability or patching issue. Instead, the attack appears to have exploited weaknesses in the process used to verify and respond to requests for IT support. A caller was able to persuade an employee to facilitate access to the organisation's single sign-on (SSO) environment without an additional verification step. Measures such as hardware security keys, callback verification, or out-of-band confirmation could potentially have provided additional safeguards between the social-engineering attempt and access to the SSO session.

The chain

- ShinyHunters placed a voice-phishing (vishing) call to an ADT employee, posing as internal IT support.
- The call talked the employee through authorising access on their Okta single sign-on (SSO) account, the identity system ADT used to gate access to its internal applications.
- That one compromised SSO session was sufficient on its own to grant the attacker full access to ADT's Salesforce environment; no additional exploit or credential theft was required.
- ADT detected the intrusion on April 20, 2026 and terminated the attacker's access, but data had already been exfiltrated by that point.

After ADT declined to pay, ShinyHunters published an 11GB archive of the stolen data on its dark-web leak site. [14]

Attacker poses as
IT support, calls an
ADT employee
(vishing)

Employee's Okta
single-sign-on
account is taken
open

One compromised
SSO session grants
full access to
ADT's Salesforce
environment

Data quietly
exfiltrated before
April 20, 2026

Ransom refused —
an 11GB archive of
stolen data dumped
publicly by
ShinyHunters

The “Low-Severity” Problem

Storm-3138 / Klue (June 2026)

Microsoft’s July 2026 threat-intelligence disclosure mapped a full year of related Salesforce intrusions (at Salesloft [2025], Gainsight, and, most recently, the market-intelligence platform Klue) back to the same underlying tradecraft, attributed most recently to the threat actor Storm-3138. Rather than stealing a password, the attackers targeted the trust relationship between a user and a connected application.

The Chain

- A vishing call talked a victim employee through Salesforce’s OAuth consent screen, presenting an attacker-controlled application disguised as Salesforce’s own “Data Loader” integration tool.
- Once the employee clicked “Allow,” the fraudulent app inherited real API permissions as that user; no password was stolen or replayed, and conventional authentication monitoring saw nothing unusual.
- With that access, the attackers enumerated and queried CRM records at will, and used what they found to hunt for credentials that could open doors into other connected SaaS platforms.
- Microsoft’s analysis provides a useful basis for including this case because incidents initially viewed as separate vendor breaches can appear more closely connected when examined through the broader pattern of OAuth abuse. [15]

Vishing call talks
an employee
through
Salesforce's OAuth
consent screen

Employee
authorises a fake
connected app

App inherits real
API permissions
and queries CRM
records — no
password needed

Attacker
enumerates and
queries CRM
records, hunts for
further credentials

Same pattern
reused across
Salesforce,
Gainsight and Klue
(2025–2026)

The “Low-Severity” Problem

McKesson (August 2026)

The largest named entry in this campaign family closed out the summer. McKesson, one of the largest U.S. healthcare distributors, disclosed unauthorised third-party application access on August 28, 2026, after ShinyHunters had already begun exfiltrating data from its Salesforce and Snowflake environments.

The Chain

- Roughly 1TB of data was pulled out over four to five days (August 21–25, 2026), including names, Social Security numbers, dates of birth, medical records and Medicaid numbers, medications, allergies and diagnoses.
- ShinyHunters demanded more than \$55 million in ransom. They claimed 284 million records, the largest claim in the campaign, though McKesson had not independently confirmed the figure at the time of the group’s disclosure. [16]

Unauthorised access gained via a trusted third-party application

Access reaches McKesson's Salesforce environment

~1TB exfiltrated over 4–5 days (Aug 21–25, 2026)

PII and health data including SSNs, diagnoses, medication and medical records

\$55M+ ransom demanded; 284M records claimed

What repeats across all three cases

Recurring pattern	Seen in	Why it works
Identity trusted over identity verified	ADT, Storm-3138/Klue	A convincing phone call or consent screen was treated as sufficient proof of who was asking.
No exploit, no malware, no CVE	ADT, McKesson	Nothing here would appear on a vulnerability scan; the entire chain lived in identity and access, not software.
Trusted third-party / connected-app access	Storm-3138/Klue, McKesson	Access was inherited through a relationship the victim organisation had already approved, not broken into from outside.

WHAT ATTACKERS PRIORITISE



What Attackers Prioritise

Defender prioritisation and attacker prioritisation address different questions. A vulnerability management programme may begin by asking, **“What are our most severe findings?”** An attacker moving through a real environment is more likely to consider, **“What is the easiest and most reliable way to reach something valuable from where I am?”** The difference is important because, as established in this report, technical severity does not necessarily reflect accessibility, exploitability, or the position of a weakness within an attack path.

What the Evidence Suggests Attackers Weigh

- **Accessibility and reliability over novelty:**

Root Evidence's Q1 2026 research found exploitation activity concentrated around a relatively small set of vulnerabilities, including vulnerabilities that had been known for several years. This suggests that attackers may favour weaknesses with established exploitation methods over newly disclosed vulnerabilities. MITRE ATT&CK reinforces this pattern by documenting how tracked threat groups repeatedly use established techniques and procedures across operations, highlighting the value of methods that are known to work. [13,11]

- **Proximity to identity and privilege:**

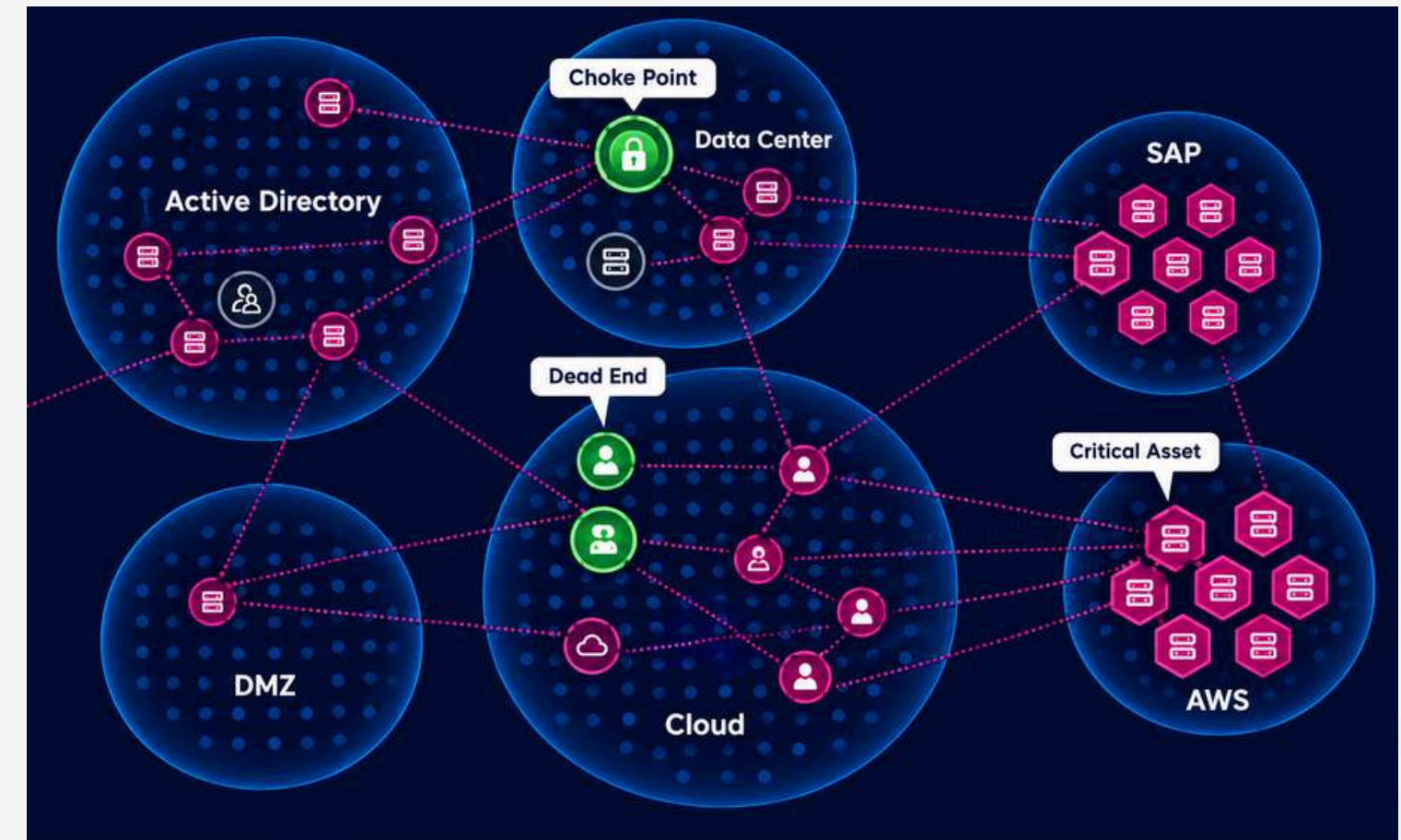
XM Cyber's research found credential- and permission-related techniques involved in 73% of the top attack techniques used against critical assets. This highlights the importance of identity, permissions and access pathways alongside conventional software vulnerabilities. [19]

- **Internet exposure and ease of initial access:**

The 2026 Verizon DBIR reported vulnerability exploitation as the leading initial-access vector, accounting for 31% of breaches examined. The finding reinforces the importance of exposure and accessibility when considering which weaknesses can provide an entry point into an environment. [12]

- **Position within an attack path:**

XM Cyber's attack-graph analysis found that a small proportion of exposures sit on “choke points” where multiple attack paths converge. Although these exposures represent a relatively small part of the overall weakness population, addressing them can affect multiple routes to critical assets. This illustrates why the position of a weakness within an attack graph can provide information that an individual severity score does not capture. [19]



Attack-path analysis identifies choke points, key intersections where multiple attack paths converge on critical assets, highlighting where remediation can have the greatest risk-reduction impact. [19]

What Attackers Prioritise

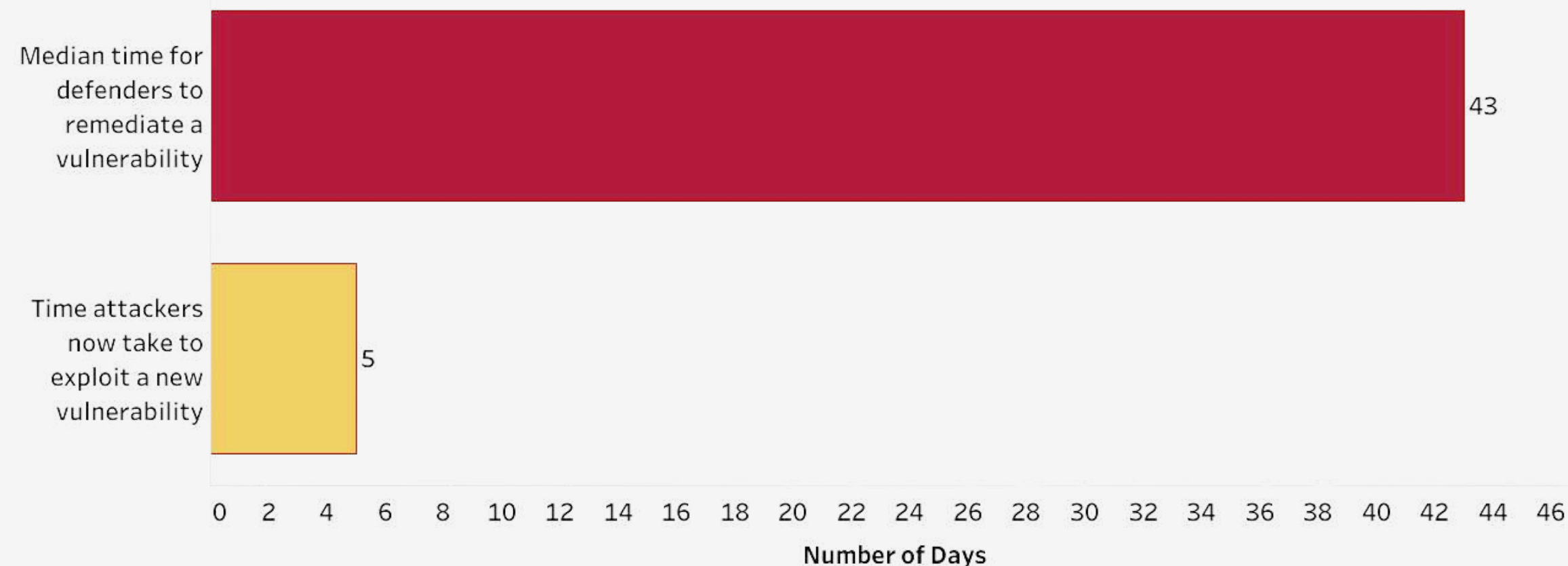
Speed Also Changes the Prioritisation Problem

The difference between attacker and defender timelines adds another dimension to the challenge. 2026 benchmark data placed the median time to fully remediate a vulnerability at approximately 43 days, while other research cited in this report places the time between disclosure and exploitation at roughly five days for some newly disclosed vulnerabilities. This creates a practical gap between the time organisations may need to assess and remediate weaknesses and the time attackers may take to begin exploiting them. [12,32]

Remediation speed can also vary considerably by environment. Benchmark data indicate that technology organisations may take 74–98 days to remediate critical flaws, while public-sector organisations in the same dataset reduced critical remediation times from 86 to 52 days. For complex enterprise applications such as Java, .NET and Citrix-class systems, remediation can extend beyond five months because of compatibility testing, change control and deployment requirements.

The scale of the workload adds further pressure. Organisations reportedly receive an average of roughly 865,000 security alerts per year, while an estimated 82% carry measurable security debt and 78% report known critical vulnerabilities running in production. These conditions make it difficult to address every finding immediately and increase the importance of distinguishing between weaknesses based on their actual exposure and relevance. [20,21]

The gap between how fast attackers move and how fast most organisations can respond



Defenders now take roughly 8x longer to close a vulnerability than attackers take to start exploiting it.[20,21]

What Attackers Prioritise

From Severity to Context

This is where exploitability and attack-path analysis provide additional context to traditional severity scoring. Research associated with EPSS v3 found that prioritising a relatively small proportion of known CVEs assessed as more likely to be exploited could address a substantial share of the vulnerabilities attackers actually use. Similarly, research that incorporates runtime environment and business importance found that only 18% of vulnerabilities initially classified as critical retained that classification when additional context was considered. [33,34]

Taken together, these findings suggest that vulnerability prioritisation involves more than identifying the highest CVSS scores. Accessibility, exploitability, identity and privilege relationships, proximity to critical assets, and the position of a weakness within an attack path can all affect its practical significance.

What makes a weakness attractive to attackers: accessibility, ease of exploitation, access gained, and proximity to valuable assets, as reflected in the figures below.

The Rising Volume of Reported Vulnerabilities (2020–2026)

More vulnerabilities. Greater prioritisation pressure.



The graph shows a substantial increase in the volume of reported vulnerabilities between 2020 and 2026, rising from 19,249 to 69,922 over the period. [2]

Recommendations

From Vulnerability Management to Attack-Path Management

The practical response to the Exploitability Gap is a shift in focus: from individual vulnerabilities to the attack paths they enable. Gartner's Continuous Threat Exposure Management (CTEM) framework reflects this approach through five recurring stages (scoping, discovery, prioritisation, validation and mobilisation) designed to assess exposure, accessibility and exploitability rather than simply score vulnerabilities. [28,30]

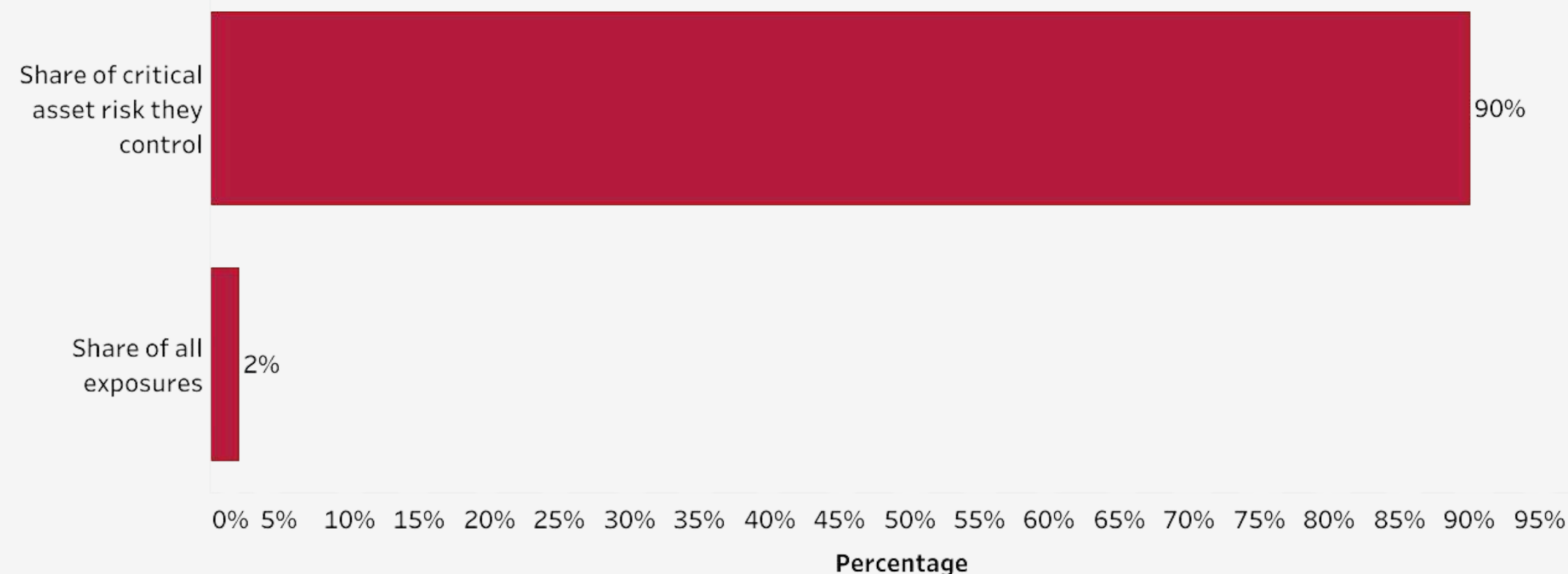
Why choke points matter

Attack-graph research from XM Cyber and the Cyentia Institute provides a practical basis for this shift. It identifies "**choke points**" as nodes where multiple attack paths converge before reaching critical assets. Remediating these points can therefore disrupt multiple attack paths at once.

- Only **2% of mapped exposures** sit on choke points; the remainder lead to dead ends that do not reach critical assets.
- Remediating that 2% can eliminate routes to **more than 90% of critical assets** across the environments studied, according to XM Cyber's analysis. [18]

The implication is that organisations may be able to achieve greater risk reduction by targeting a relatively small number of strategically important weaknesses rather than attempting to remediate the entire vulnerability backlog.

A small, identifiable fraction of exposures controls the large majority of critical-asset risk



Just 2% sit on the "choke points" where attack paths converge, yet remediating that 2% eliminates the routes to over 90% of critical assets. [18]

Recommendations

The projected payoff and the current gap

Gartner has projected that, by 2026, organisations prioritising security investment through continuous exposure management could be **three times less likely to suffer a breach** than those that do not. Adoption remains uneven, however. A 2026 industry survey found that **96% of security teams struggle to validate whether an exposure is exploitable in their environment**, while two in three lack a consolidated view of their overall exposure. [26,27]

Taken together, the evidence from CVSS-exploitation research, breach investigations, attack-graph analysis and real-world cases suggests that vulnerability severity alone does not provide sufficient context for remediation. Closing the Exploitability Gap therefore means identifying the weaknesses that attackers can actually reach, combine and use to access critical assets, and prioritising remediation according to the attack paths they enable. This shifts vulnerability management from simply ranking individual weaknesses to identifying and disrupting the small number of exposures, permissions, identities and misconfigurations that allow multiple attack paths to converge on critical assets. [25]

What this suggests for security leaders

- **Use CVSS as one input, not the sole trigger.**

Combine severity with confirmed exploitation signals such as CISA KEV and EPSS before prioritising remediation.

- **Expand vulnerability management beyond CVEs.**

Include identity, credential, permission and configuration weaknesses that can form part of an attack path.

- **Identify choke points.**

Use attack-path or exposure-graph analysis to find weaknesses whose remediation can disrupt multiple routes to critical assets.

- **Use security controls as chain-breakers.**

Apply MFA, out-of-band verification, least-privilege IAM and lateral-movement detection across the access points attackers can chain together.

- **Measure remediation speed as a risk metric.**

Where vulnerabilities can be weaponised faster than organisations typically remediate them, automation, reachability analysis and tighter SLAs become important to reducing exposure.

- **Continuously validate whether attack paths remain open.**

Reassess critical attack paths after remediation, configuration changes and new exposures to confirm that previously identified routes to critical assets have actually been disrupted. This helps ensure that remediation reduces exploitable exposure rather than simply closing individual findings.

Sources

1. [CVE — Related Efforts](#)
2. [NIST National Vulnerability Database \(NVD\) — Vulnerability Statistics](#)
3. [CISA — Known Exploited Vulnerabilities \(KEV\) Catalog](#)
4. [Brandefense — “Why CVSS Scores Are Lying to Your Security Team”](#)
5. [Picus Security — “Vulnerability Prioritization in 2026: Why CVSS Isn’t Enough”](#)
6. [Axis Intelligence — “CISA KEV Statistics 2026: 1,665 Entries, 3-Day Clock”](#)
7. [MITRE ATT&CK — Enterprise Tactics](#)
8. [MITRE ATT&CK — Initial Access \(TA0001\)](#)
9. [MITRE ATT&CK — Credential Access \(TA0006\)](#)
10. [MITRE ATT&CK — Privilege Escalation \(TA0004\)](#)
11. [MITRE ATT&CK — Frequently Asked Questions](#)
12. [Verizon — 2026 Data Breach Investigations Report \(DBIR\)](#)
13. [Root Evidence — Q1 2026 Report](#)
14. [Security Boulevard / Strokes — “Top 10 Data Breaches of April 2026”](#)
15. [SQ Magazine — “ShinyHunters Abuses Salesforce OAuth to Bypass MFA”](#)
16. [HIPAA Journal — “ShinyHunters Claims Theft of 284M Records from Healthcare Giant McKesson”](#)
17. [XM Cyber — “80% of Security Exposures Are Fueled by Misconfigurations”](#)
18. [XM Cyber — “Small Number of Exposures Put More Than 90% of Critical Assets at Risk”](#)
19. [XM Cyber — “Navigating the Paths of Risk: The State of Exposure Management in 2024”](#)



Sources

20. [Endor Labs — “Mean Time to Remediate \(MTTR\): How to Measure It and Cut It”](#)
21. [Pixee — “Vulnerability Remediation Statistics 2026”](#)
22. [The Hacker News — “N-able Issues Fourth N-central Hotfix in Five Weeks for Unauthenticated RCE Flaw” \(CVE-2026-86206 / 86207 scores\)](#)
23. [The Hacker News — “N-able N-central Pre-Auth RCE Flaw Exploited in the Wild” \(Rapid7 chain\)](#)
24. [The Hacker News — “LiteLLM Flaw CVE-2026-42271 Exploited in the Wild, Chains to Unauthenticated RCE”](#)
25. [Kodem Security — “Context Over CVSS: Why Medium, Low CVEs Matter More Than You Think”](#)
26. [Splunk — “Continuous Threat Exposure Management \(CTEM\)”](#)
27. [SimSpace — “Gartner’s CTEM Trend Explained for Real Security Teams”](#)
28. [ArmorCode — “The Ultimate Guide to Continuous Threat Exposure Management \(CTEM\) in 2026”](#)
29. [The Hacker News \(Expert Insights\) — “Why Threat Intelligence Is the Missing Link in CTEM Prioritization and Validation”](#)
30. <https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025>
31. <https://www.first.org/epss/>
32. <https://www.tenable.com/blog/cyber-risk-lurks-in-the-vulnerability-disclosure-gaps>
33. <https://www.securityscientist.net/blog/cvss-vs-epss/>
34. <https://www.datadoghq.com/about/latest-news/press-releases/datadog-state-of-devops-2025/>



THE CYBERKACH LEARNING MANAGEMENT SYSTEM

From onboarding to ongoing awareness, the Cyberkach LMS turns cybersecurity training into a measurable, manageable part of how your organisation runs, not a once-a-year checkbox.

- ✓ Role-based training content
- ✓ Realistic phishing simulations
- ✓ Instant dashboards and reporting
- ✓ Department & group-level insights
- ✓ Built for teams of any size

EXPLORE THE LMS

cyberkach.com/lms



Practical learning. Clear progress. Confident teams.

Contact us

For further insights or expert interpretation, speak with our team. We help organisations translate threat intelligence into actionable insights. Reach out to us to continue the conversation and explore your next steps.

Email

hello@cyberkach.com

Website

www.cyberkach.com

LinkedIn

[Linkedin.com/company/cyberkach](https://www.linkedin.com/company/cyberkach)

