# Surge in cybersecurity threats raises alarm as CVEs increase by 30%



In a marked increase in cybersecurity threats, reported Common Vulnerabilities and Exposures (CVEs) have surged by 30% this year. Security Magazine highlights that the success of cyber attacks that leverage these vulnerabilities often does not rely solely on exploiting new zero-day flaws. Many entities have been slow to respond to published CVEs, resulting in a notable 10% escalation in the exploitation of older vulnerabilities by threat actors. This delay provides hackers with ample opportunity to execute attacks on outdated systems when proactive measures are lacking.

A pressing example is the case of Fortinet, which revealed that approximately 86,000 instances of its software remained exposed to a significant vulnerability (CVE-2024-23113) that attackers began to exploit after it had been on the radar for nearly nine months. The incident underscores a broader challenge facing security teams, who must balance the immediate need for patching production systems against the risks inherent in rapid implementations without proper testing. With limited bandwidth and ongoing threats, these teams often find themselves in a continuous cycle of responding to incidents as they arise.

The need for robust cybersecurity practices extends beyond an organisation's immediate systems. Key attention must also be placed on the interconnected ecosystem involving partners, suppliers, and vendors. Many organisations are not fully aware of the security measures these external entities have instituted, leaving them vulnerable to risks that can propagate through their networks. A lack of confidence in the security protocols of external partners often leads to a frantic scramble for emergency assessments when threats emerge.

Recent incidents, such as the disruption caused by CrowdStrike’s security breach affecting Microsoft Windows, illustrate the broader implications of cybersecurity failures. Major operational disruptions ensued, resulting in canceled flights, halted medical procedures, and delayed financial transactions. Past events, including the Log4j vulnerabilities, have similarly led to widespread chaos, impacting critical systems like payroll processing and educational institutions. The ramifications of such incidents can entail billions of dollars in losses from operational impacts, ransomware payments, litigation costs, and recovery efforts.

As the volume of reported CVEs continues to rise, cybercriminals are seizing opportunities created by vulnerabilities in the software supply chain, leading to increased notoriety and financial gains for these groups. This situation places immense pressure not only on security teams but also on procurement and compliance sectors to effectively manage third-party risks.

To mitigate these threats, security leaders must adopt a strategic approach to threat management. Essential steps include enhancing visibility into emerging threats, utilising resources such as the CISA’s Known Exploited Vulnerabilities (KEV) catalog or NIST’s National Vulnerability Database (NVD) to receive timely alerts on vulnerabilities. It is also crucial to identify which vendors and third parties may be susceptible. Security leaders are encouraged to categorise their third-party ecosystem from the least critical to the most essential, thereby streamlining assessments of risk as threats emerge.

The process requires targeted assessments rather than blanket approaches; these assessments should focus specifically on threats relevant to particular vendors without overwhelming them with unnecessary requests. Enhanced communication and transparency during high-stakes scenarios are critical to reassure senior leaders, customers, and partners that the security team is actively managing incidents.

Despite the complexity of rapidly responding to cybersecurity incidents—which can take days or even months—there are opportunities for security leaders to speed up and streamline their processes. By doing so, they can enhance their organisations' resilience, ultimately reclaiming valuable time and resources to focus on critical areas of security strategy and improvement.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.f5.com/labs/articles/threat-intelligence/the-evolving-cve-landscape> - Corroborates the increasing number of CVEs and the growing rate of CVE publication, highlighting a 10% annual growth and the expectation of 547 new CVEs per week by 2025.
2. <https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one> - Supports the surge in reported CVEs, noting 26,447 vulnerabilities disclosed in 2023, and highlights the quick exploitation of high-risk vulnerabilities, often within days of publication.
3. <https://www.indusface.com/blog/key-cybersecurity-statistics/> - Provides statistics on the increase in CVEs, including a 30% jump in 2024 compared to 2023 and an average of 115 CVEs disclosed daily, underscoring the growing attack surface.
4. <https://www.cybersecuritydive.com/news/cve-exploitation-tripled-2023-verizon/714848/> - Details the nearly tripled exploitation of vulnerabilities in 2023, emphasizing the challenge of patching and the role of third-party vulnerabilities in breaches.
5. <https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one> - Highlights the exploitation of older vulnerabilities and the short window for response, with 25% of high-risk CVEs exploited on the day of publication and 75% within three weeks.
6. <https://www.cybersecuritydive.com/news/cve-exploitation-tripled-2023-verizon/714848/> - Mentions the MOVEit breach and the exploitation of zero-day vulnerabilities, illustrating the impact of delayed patching and the importance of third-party risk management.
7. <https://www.f5.com/labs/articles/threat-intelligence/the-evolving-cve-landscape> - Discusses the broader challenge of balancing patching needs with the risks of rapid implementations, reflecting the ongoing cycle of responding to incidents.
8. <https://www.indusface.com/blog/key-cybersecurity-statistics/> - Emphasizes the need for robust cybersecurity practices beyond immediate systems, including attention to the security measures of external partners and vendors.
9. <https://www.cybersecuritydive.com/news/cve-exploitation-tripled-2023-verizon/714848/> - Highlights the impact of cybersecurity failures on operational systems, such as the disruption caused by breaches affecting critical systems like payroll processing and educational institutions.
10. <https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one> - Supports the importance of using resources like CISA’s Known Exploited Vulnerabilities (KEV) catalog and NIST’s National Vulnerability Database (NVD) for timely alerts on vulnerabilities.
11. <https://www.cybersecuritydive.com/news/cve-exploitation-tripled-2023-verizon/714848/> - Underlines the necessity for targeted assessments and enhanced communication during high-stakes scenarios to manage incidents effectively and reassure stakeholders.
12. <https://www.securitymagazine.com/articles/101271-mitigating-cve-exploitations-putting-the-rapid-into-rapid-response> - Please view link - unable to able to access data