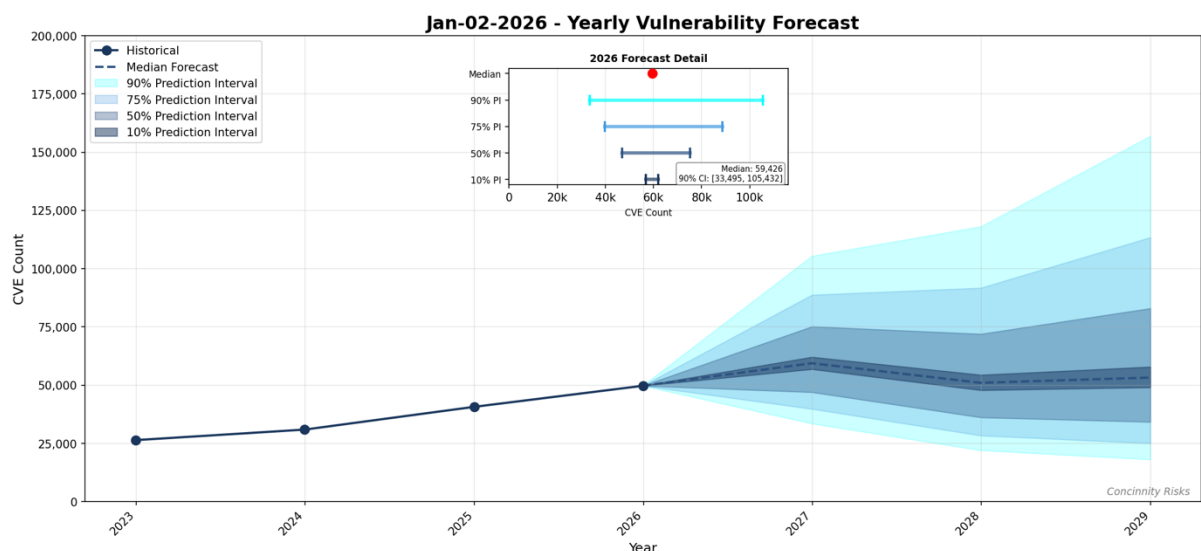# FIRST Releases 2026 Vulnerability Report, Projecting Record-Breaking Common Vulnerabilities and Exposures

For the first time ever, annual CVE disclosures expected to surpass 50,000, signaling a potential paradigm shift in vulnerability management workloads

FEBRUARY 11, 2026 - [The Forum of Incident Response and Security Teams](#) (FIRST), a leading global cybersecurity nonprofit, today released its [2026 Vulnerability Forecast](#), predicting a median of approximately 59,000 new Common Vulnerabilities and Exposures (CVEs) this year, while also marking the first time the industry will cross 50,000 published CVEs in a single year. The upper bound of FIRST's 90% confidence interval approaches 118,000, underscoring the urgent need for organizations to scale their security operations and prioritize strategically.

Key findings from FIRST's 2026 Vulnerability Forecast include:

- A median forecast of approximately **59,427 CVEs in 2026**, with a 90% confidence interval ranging from 30,012 to 117,673

- 2026 will be the **first year to exceed 50,000 published CVEs**, representing a significant milestone in vulnerability disclosure history

- Realistic scenarios suggest **70,000 to 100,000 vulnerabilities** are entirely possible this year

- The **three-year outlook** projects continued growth: 51,018 CVEs (median) in 2027 and 53,289 CVEs (median) in 2028, with upper bounds reaching nearly 193,000 by 2028

- FIRST's 2025 forecast achieved a **Mean Absolute Percentage Error (MAPE) of 7.48%** for yearly predictions and 4.96% for Q4, demonstrating the reliability of its methodology

"The question organizations need to ask right now is: are my people and processes ready to handle this volume, and am I prioritizing the vulnerabilities that actually put my data at risk? Our forecast allows defenders to stop reacting to every new CVE and start making strategic decisions about where to focus limited resources before attackers exploit the gaps," said Éireann Leverett, FIRST Liaison and Lead Member of FIRST's Vulnerability Forecasting Team.

Why These Numbers Matter

The forecast serves as a critical planning tool for security teams across the industry. Whether organizations are planning patching capacity, writing coordinated vulnerability disclosure reports, or developing detection signatures for SIEM, EDR, or IDS platforms, understanding the expected volume of vulnerabilities enables better resource allocation and strategic decision-making.

"Much like a city planner considering population growth before commissioning new infrastructure, security teams benefit from understanding the likely volume and shape of vulnerabilities they will need to process," Leverett added. "The difference between preparing for 30,000 vulnerabilities and 100,000 is not merely operational, it's strategic."

Recommendations for Organizations

With a potentially record-breaking year ahead, organizations should:

- **Assess capacity now**: Evaluate whether current people and processes can handle 50,000+ CVEs

- **Prioritize ruthlessly**: Focus on vulnerabilities that pose the greatest risk to your specific environment, not just those with the highest CVSS scores

- **Plan for scenarios**: Prepare for the median forecast but build contingency plans for higher-volume scenarios

- **Leverage forecasting**: Use vulnerability forecasts alongside asset inventories to make vendor- and product-specific preparations

"No company can solve vulnerabilities and cybersecurity in isolation. The organizations that recover fastest are the ones with trusted networks already in place, sharing threat intelligence and coordinating response before a crisis hits," said Chris Gibson, CEO, FIRST.

Looking Ahead

Throughout 2026, FIRST will publish quarterly forecast updates that refine predictions as new data arrives. These updates will incorporate more granular analysis, including expected CVSS v3 vector distributions, helping organizations understand not just how many vulnerabilities to expect, but what kinds. To learn more about FIRST's CVSS, go to: https://www.first.org/cvss/

METHODOLOGY:

The FIRST 2026 Vulnerability Forecast employs a new statistical model optimized to reflect the range of possible outcomes rather than point prediction accuracy alone. The model accounts for the structural change in CVE publication patterns that occurred in 2017-2018, providing asymmetric confidence intervals that acknowledge the higher probability of exceeding median forecasts. Data sources include historical CVE records and publication trends from the National Vulnerability Database (NVD) and MITRE.

Issued on behalf of FIRST. For further information, please contact FIRST Press.

About FIRST

FIRST aspires to bring together incident response and security teams from every country across the world to ensure a safe internet for all. Founded in 1990, the Forum of Incident Response and Security Teams (FIRST) consists of internet emergency response teams from more than 800 corporations, government bodies, universities and other institutions across 110 countries in the Americas, Asia, Europe, Africa, and Oceania. For more information and to see the full calendar of events, visit: FIRST.Org.

Connect with FIRST on social media via BlueSky, GitHub, LinkedIn, Mastodon, Meta, X and YouTube.