MONTHLY THREAT REPORT

JANUARY

2026

MISBAR

Executive Summary

We are pleased to present this comprehensive report tracking the pivotal Cyber Security events of 2026. This summary covers the full landscape of ***January and the first half of February***, highlighting the most significant threats, data breaches, and technological shifts that have defined the start of this year.

This report is a collaborative effort by the Misbar Team, dedicated to providing deep insights and analytical clarity. Our goal is to empower professionals and enthusiasts alike to stay ahead of the rapidly evolving digital frontier.

Connect With Us:
Stay updated with real-time alerts and upcoming technical deep-dives through our official channels:

X: @MisbarSec
WhatsApp Channel: Follow us

2026 Cyber Landscape: A Rapidly Expanding Attack Surface

As of February 15th, 2026, the digital threat landscape has accelerated at an unprecedented pace. The first six weeks of the year have already seen the publication of ***7,620*** vulnerabilities representing a sharp ***43%*** increase compared to the same period last year.

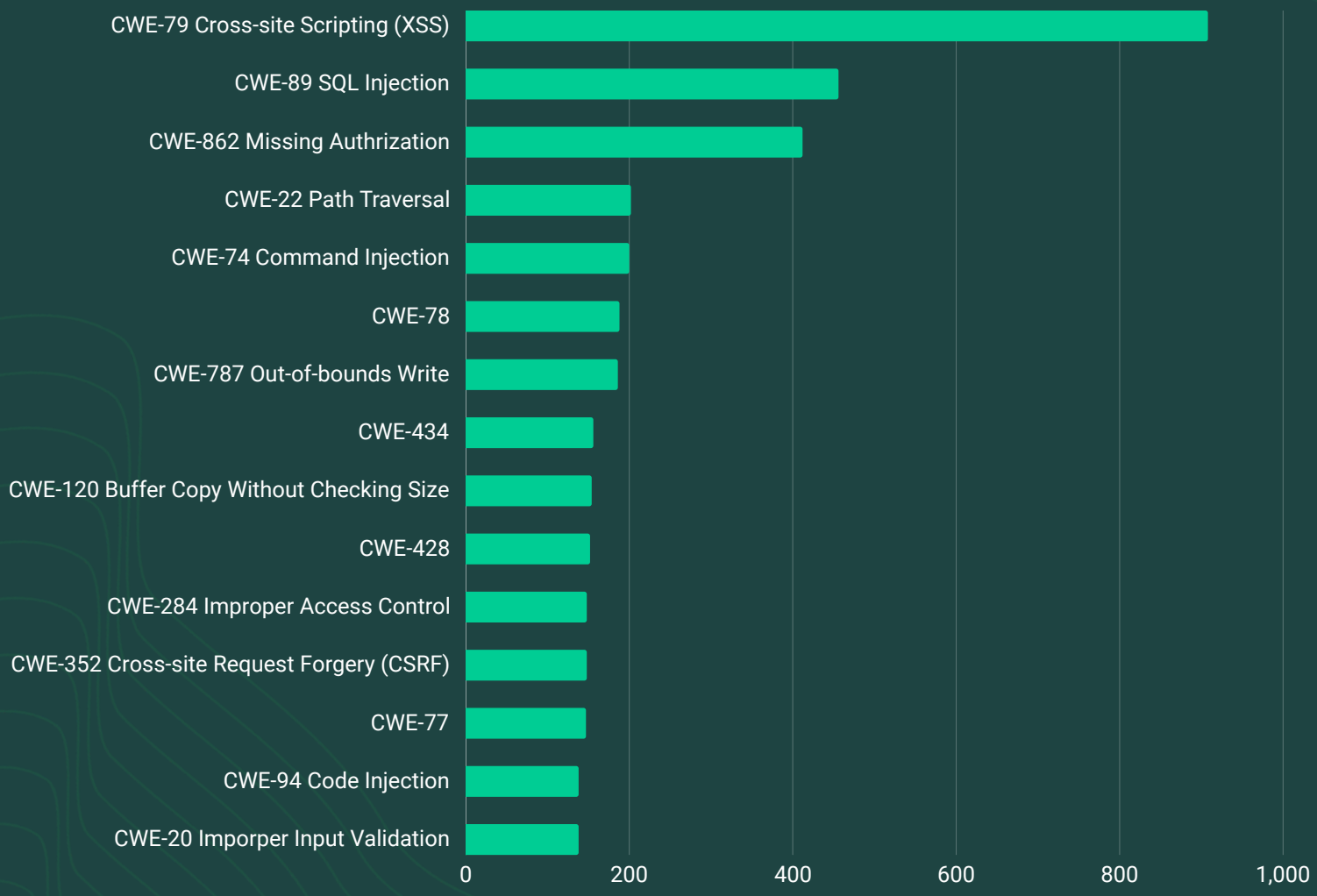
With an average of ***169%*** new vulnerabilities surfacing each day, the pressure on security teams to patch and protect has never been higher. This report, provides a breakdown of these threats from January through mid-February to help you navigate this volatile environment.

CRITICAL	**971**
HIGH	**2,532**
MEDIUM	**2,545**
LOW	**151**
N/A	**1,390**

Severities are evaluated based on CVSS scoring ranging between 0-10. NA means scoring between zero and two.

Dominant Threats: The CWE Landscape

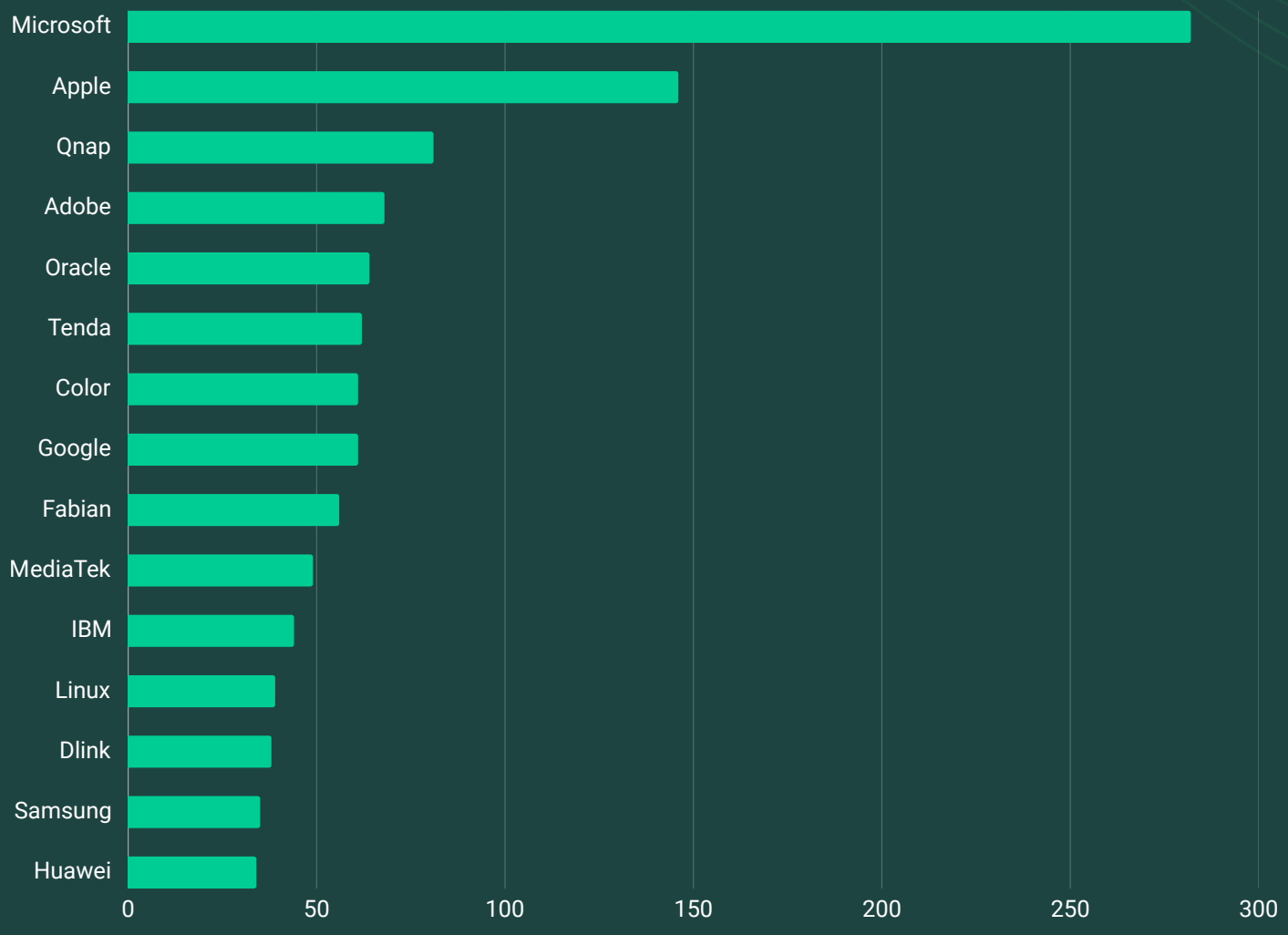
The opening of 2026 reveals a persistent focus on both classic and structural weaknesses. While CWE-79 (Cross-Site Scripting) remains the most frequent discovery, there is a concerning surge in high-impact flaws like CWE-787 (Out-of-Bounds Write) and CWE-862 (Missing Authorization). This shift indicates that while volume remains high in web-based vulnerabilities, attackers are increasingly finding success in exploiting deep-seated memory safety issues and broken access controls.



Top Common Weaknes Enumration vulnerability types

Top Affected Vendors

The first six weeks of 2026 highlights a significant concentration of vulnerabilities within major industry leaders. Microsoft leads the list by a substantial margin, followed by other key infrastructure and hardware providers like Qnap and Oracle. This trend underscores that attackers and researchers are heavily focused on high-impact platforms, emphasizing the critical need for robust patch management and proactive defense for organizations relying on these widely deployed technologies.



Top Affected Vendors

Conclusion

As we conclude this review of January and the first half of February 2026, the data paints a clear picture of an intensifying cyber environment. With ***7,620*** vulnerabilities already published a ***43%*** increase over the previous year the rapid pace of discovery (averaging ***169%*** new vulnerabilities daily) demands heightened vigilance. The dominance of CWE-79 (XSS) and the high volume of flaws affecting major vendors like Microsoft and Qnap serve as a reminder that both web applications and core infrastructure remain primary targets. Misbar Team remains committed to monitoring these developments to keep you informed and secure.