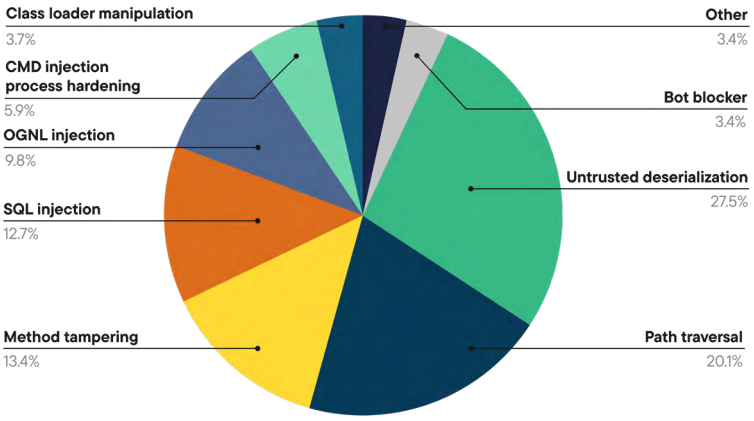
# AppSec Overflow 2026

## AppSec math is broken, and AI is the reason

Runtime telemetry from inside thousands of production applications and APIs shows exactly where the numbers stopped working and what defenders can do about it.

### Where the application vulnerabilities are

- **42 viable attacks per application every month:** Confirmed exploitation attempts that reached and triggered real vulnerabilities in running code
- **One attack every four minutes:** The average application absorbs 11,382 attacks per month
- **22 serious vulnerabilities per app, 3.4 fixed per month:** Critical vulnerabilities take an average of 92 days to remediate
- **54% of observed CVEs are more than a year old:** Spring4Shell and Log4Shell both remain widely present in production four years after disclosure
- **AI scanners agree with each other 5% of the time:** One scanner run three times against the same code reproduced only 17% of its own results




### The find-and-fix model is running out of room

For two decades, application security has followed the same sequence: find vulnerabilities, prioritize them, patch them before an attacker arrives. That sequence depends on defenders absorbing the volume of findings and patching faster than attackers can weaponize.

AI has broken both assumptions at once. Vulnerability discovery has been industrialized while remediation capacity stayed flat, and the window from disclosure to exploitation has collapsed from years to hours.

### Get the full report to learn

- Attack volume and technique breakdowns from production environments, including how viable attack patterns shift across finance, healthcare, manufacturing, services and technology
- Contrast Labs research on the cost, consistency and reproducibility of AI security scanners
- Vulnerability findings per application, remediation throughput, third-party CVE aging analysis, and the high-prevalence CVEs still active years after disclosure
- Where CVSS, EPSS and CISA KEV overlap, where they diverge, and why neither severity nor exploit probability is sufficient alone

**Download the full report**

Contrast Security is the world's leader in Runtime Application Security, embedding code analysis and attack prevention directly into software. Contrast's patented security instrumentation enables powerful Application Security Testing and Application Detection and Response, allowing developers, AppSec teams and SecOps teams to better protect and defend their applications against the ever-evolving threat landscape.



**contrastsecurity.com**

6800 Koll Center Parkway
Ste 235
Pleasanton, CA 94566
Phone: 888.371.1333