Black Duck Newsroom

# Newly Discovered Software Vulnerabilities Outpace Fixes 18 to 1 as Exploit Windows Shrink, New Black Duck Research Shows

*The report highlights that closing the gap takes deterministic testing, AI-assisted triage and agentic remediation working together.*

BURLINGTON, Mass., Nov. 17, 2026 /PRNewswire/ -- Black Duck®, the leader in application security for the AI era, today released its *2027 AI Readiness Report*, which shows that the gap between finding vulnerabilities and fixing them is widening just as AI shortens the time attackers need to exploit them. Based on 65.5 million application security testing findings, the report finds that most organizations are finding vulnerabilities at an unprecedented scale, but only a small share of what they find is fixed in a timely manner.

Security teams used to have time on their side, but the Zero Day Clock data shows that the average span between a vulnerability's disclosure and its first exploit has fallen from 2.6 years in 2018 to under one day today. Black Duck's report says frontier AI models are accelerating the trend, and that the traditional model of finding a flaw, assessing it and scheduling a fix no longer fits that timeline.

Key findings include:

**Discovery Is Outpacing Remediation**

In June 2025, organizations in the report identified 11 new findings for every one they closed, and by May 2026 that ratio was 18 to 1 after peaking at 22 to 1 in December. By the end of the study period, only about 1 in 10 findings (10.5%) had been closed. This is an operational-scale problem, and even doubling remediation capacity would leave the backlog growing.

The vulnerabilities that do get fixed still take weeks. Flaws found in proprietary code through static application security testing (SAST) took a median of 28 days to close, and open source vulnerabilities found through software composition analysis (SCA) took 39 days. Issues surfaced by dynamic and manual testing took far longer, at 316 and 232 days, respectively. Against an exploit window of under a day, the report says a vulnerability left open for weeks is no longer a routine backlog item but an open window.

**The Most Severe Open Source Vulnerabilities Aren't Being Fixed First**

When vulnerabilities arrive by the millions, the most serious ones are not always fixed first. Among closed open source vulnerabilities, critical-severity issues took a median of 58 days, compared with 22 days for high-severity ones, suggesting that teams may be clearing what's easiest, not what's most dangerous.

The stakes are high because much of the serious risk sits in code organizations didn't write, with open source and third-party components accounting for 52% of all critical- and high-severity vulnerabilities. Across all vulnerabilities SCA identified, only 15% had been closed.

Severity alone can't close the gap, because it is an incomplete guide to risk. In advisories Black Duck published in 2025, known exploits existed for 45% of high-severity vulnerabilities, 39% of medium-severity vulnerabilities and 31% of low-severity vulnerabilities. Since AI can combine several minor weaknesses into one serious attack,

organizations must weigh exploitability, reachability and business context alongside severity.

**Closing the Gap Will Take Agentic Remediation That Works at Machine Speed**

Deciding what to fix first across millions of vulnerabilities is more than any team can do manually. The organizations that closed vulnerabilities fastest tended to scan more often. Those running SCA scans 10 to 29 times a month closed open source vulnerabilities in an average of 30 days, compared with 66 days for those scanning less than monthly.

The report's answer is to fix vulnerabilities faster than attackers can exploit them, and that takes three layers working together. Deterministic testing finds vulnerabilities with consistent, auditable results. AI-assisted triage prioritizes them, weighing exploitability, reachability and business context to decide what to fix first. Agentic remediation then fixes, with AI generating and validating fixes that developers review and approve.

"Attackers now move from disclosure to exploit in less than a day, and most organizations still need weeks to ship a fix. That math doesn't work. Finding vulnerabilities is no longer the hard part. Organizations are finding 18 for every one they fix, and adding more scanners or more people won't close that gap," said Greg Hughes, chief executive officer at Black Duck. "The organizations that win will find, prioritize, and fix at machine speed, using deterministic testing they can trust, AI that knows what matters and agentic remediation that closes the loop. Boards and regulators will judge organizations on time to fix, not on how many vulnerabilities they found."

**About the Research**

The data reflects aggregated, anonymized telemetry from Black Duck customers, analyzing 65,521,627 vulnerabilities identified through SAST, SCA, dynamic application security testing and manual application security testing across 13,127 applications at 533 organizations, collected from June 2025 through May 2026. Time-to-close figures cover only vulnerabilities that were closed during the study period. The dataset comprises organizations that have invested in commercial application security tooling and may have higher baseline maturity than the broader market.

To learn more, download the 2027 AI Readiness Report.

**About Black Duck**

Black Duck® is application security for the AI era. Our approach is hybrid by design. Deterministic analysis delivers verifiable results and serves as the system of record for governance, while AI-powered reasoning prioritizes what's exploitable and agentic remediation fixes it at machine speed — so your team ships as fast as AI writes code, without inheriting the risk that comes with it. Trusted by thousands of organizations in many of the world's most demanding industries, including aerospace, defense, automotive, semiconductor, and healthcare, and backed by more than 20 years of human-verified vulnerability intelligence. Learn more at www.blackduck.com.

SOURCE Black Duck Software

For further information: Mark Van Elderen, Black Duck, 650.793.7450, mvanelde@blackduck.com

---

Exploit-Windows-Shrink,-New-Black-Duck-Research-Shows