Five AppSec risks that threaten your business

A single weak point in a line of code can create an open door for attackers.

Are you protected from these common risks?

**Risk 1: Dependence on open source**
- Weakness in open source components can spell disaster.
- In 2017, 83% of applications were found to have at least one critical or high vulnerability.
- The longer vulnerabilities remain unpatched, the cost of remediation increases.

**Risk 2: Lengthy exposures**
- There are often big gaps between vulnerability discovery and patch availability.
- Even with a prompt patch management program, vulnerabilities can persist for months or years.

**Risk 3: Costly remediation**
- Every day a vulnerability remains unpatched, costs can escalate.
- The production/post-release phase is 30x more expensive to remediate than vulnerabilities found earlier in the lifecycle.

**Risk 4: Repeated security flaws**
- Many software teams continue to make the same mistakes, such as input validation errors.
- Between 2016 and 2017, as more companies integrate and automate security, the number of remediated issues increased by more than 30%.

**Risk 5: Applications not integrated with DevOps**
- Software security should be integrated with DevOps to ensure quality and speed of remediation.
- In 2017, over 87% of vulnerabilities found through static application security testing (SAST) were remediated within 30 days and over 80% were fixed within 15 days.

Don’t bet your business on risky software. Take control today.

**Software security checklist**
- Scan all your code—on demand or on premises—with Micro Focus Fortify.
- Use AppSec testing to find and fix vulnerabilities proactively.

LEARN MORE

2 This is the 2017 update on data collected through 2016.
3 National Institute of Standards and Technology

© 2017 Micro Focus. All rights reserved.

Java is a registered trademark of Oracle and/or its affiliates.

a00018217ENW, Rev. 1, September 2017