DATA SHEET

azul

Your Patch Cycle Was Designed for a Slower Enemy

Your application has already been exploited – you just don't know it yet

New AI frameworks like Anthropic's Claude Mythos can find and create exploits for vulnerabilities even before they're disclosed. This has fundamentally changed the software industry:

#1 Initial Vector of Attack: Vulnerability Exploitation
Replacing email phishing and credential theft

MTTE: *-1 Days*
Mean Time To Exploit a known vulnerability is now measured in negative days

If you're using unsupported Java, you may not be aware that you only have access to **quarterly Patch Set Updates (PSUs)**, which OpenJDK vendors typically make available days to weeks after Oracle. And because PSUs include hundreds of bug fixes, security updates, new features, and more, they **require days of testing before deployment.**

The window between Common Vulnerabilities and Exposures (CVE) publication and active weaponization has collapsed due to AI. "Best effort" patching is no longer a viable posture – it's a multi-million dollar liability.

The New Attack Timeline

T0 → Vulnerability exists

Flaw is present in production systems. No disclosure yet. AI tools may have already found it and created an exploit allowing hackers to start probing at scale.

T0 +hours → Oracle releases their quarterly update followed by Azul; CVEs are published

Public disclosure triggers automated exploit generation pipelines. The clock is ticking as you wait for your OpenJDK vendor's patch. The attacker's clock started earlier.

T0 +24–48hrs → Active exploitation is underway

Weaponized code is circulating. Your company's 30-day patch SLA is already a breach in progress.

T0 +30 days → Patch deployed (traditional)

By this point, organizations with "best effort" patching have been exposed for weeks.

Your Java is Only as Secure as Your JDK

Azul is the only OpenJDK vendor that helps close the gap between AI-driven vulnerability exploitation and your current patching cycle by offering:

Quarterly Critical Patch Updates (CPUs)

CPUs, delivered on a strict SLA, include only critical and security fixes deployed on the previous patch, which has been extensively tested by the community. This makes CPUs suitable for rapid deployment to quickly address the vulnerabilities disclosed in each quarterly release, as well as meet regulatory security requirements.

Out-of-cycle Updates

Out-of-cycle updates are essential to addressing zero-day vulnerabilities, as well as critical functional regression issues.

Ready to address AI-driven security risk? Contact Azul.

Azul is the trusted leader in enterprise Java for today's AI and cloud-first world. Its open source-based Java platform empowers organizations to optimize the entire Java lifecycle to accelerate performance, strengthen security, reduce licensing and cloud costs, and boost developer productivity. Azul powers mission-critical systems for 36% of the Fortune 100, 50% of the Forbes Top 10 World's Most Valuable Brands, and the world's top 10 financial trading companies. Learn more at azul.com and follow @azulsystems.

www.azul.com | +1.650.230.6500

385 Moffett Park Drive, Ste 115
Sunnyvale, CA 94089 USA