87% of Organizations Are Running Software With Known, Exploitable Vulnerabilities, Datadog Finds

February 26, 2026 at 9:15 AM EST

The State of DevSecOps Report 2026 highlights a broader industry shift as security risk increasingly moves upstream into the software supply chain

NEW YORK, Feb. 26, 2026 (GLOBE NEWSWIRE) -- Datadog, Inc. (NASDAQ: DDOG), the AI-powered observability and security platform for cloud applications, today released its latest State of DevSecOps Report, finding that nearly nine in 10 organizations (87%) have at least one known exploitable vulnerability in deployed services.

The report points to a broader industry shift, with security risk increasing across the software delivery lifecycle. As development accelerates, becomes more automated, and relies more heavily on third-party components, risk is increasingly shaped by the software supply chain and the tools used to build and deploy applications - not just the code that runs in production.

Key findings at a glance:

- 87% of organizations have at least one known exploitable vulnerability in deployed services
- 42% of services rely on libraries that are no longer actively maintained
- Services using end-of-life language versions face exploitable vulnerabilities in 50% of cases, compared to 31% for supported versions
- 50% of organizations adopt new library versions within 24 hours of release, increasing the risk of installing malicious or compromised software
- Only 4% of organizations pin all public GitHub Actions to a specific version using commit hashes, leaving CI/CD pipelines vulnerable to silent code changes

Security Risk Increasing at Both Ends of the Lifecycle

On one end, software is aging faster than teams can keep it up to date. The median software dependency is now 278 days out of date - 63 days further behind than last year.

At the same time, third-party software accelerates development but introduces risk when implicitly trusted. Datadog researchers found that half of organizations (50%) adopt new library versions within 24 hours of release, and only 4% pin all public GitHub Actions to a specific version using commit hashes.

As a result, build and deployment pipelines are increasingly exposed to silent changes in third-party code, making CI/CD systems a critical supply-chain risk.

“The way software is built has fundamentally changed, but security practices haven’t kept up,” said Andrew Krug, Head of Security Advocacy at Datadog. “DevSecOps teams are caught between moving too slowly and moving too fast. Go slow, and outdated software accumulates known vulnerabilities. Go fast, and automation can introduce unvetted code. The real challenge, though, isn’t speed - it’s clarity. As environments grow more complex, AI-assisted workflows help ensure top priorities get attention first.”

Alert Volume Is Obscuring Real Risk

While vulnerability alerts continue to rise, the report also finds that most do not represent immediate business risk. Only 18% of vulnerabilities labeled “critical” remain critical once runtime context is applied.

“When almost everything is labeled ‘critical’, nothing is,” Krug added. “Teams get paged for noise while threats that pose real risk slip through. Without context, prioritization becomes harder - leading to burnout, slower response times and accumulated risk. Teams need better visibility into what *actually* requires action.”

Read the full report, State of DevSecOps Report 2026, to see how these findings are shaping modern approaches to detecting, prioritizing and remediating security risk.

Contact
press@datadoghq.com

Report Methodology

Datadog analyzed telemetry from tens of thousands of applications to assess security risk across modern software environments, along with additional

datasets used for specific findings. The data is global in scope.

About Datadog

Datadog is the AI-powered observability and security platform for cloud applications. Our SaaS platform integrates and automates infrastructure monitoring, application performance monitoring, log management, user experience monitoring, cloud security and many other capabilities to provide unified, real-time observability and security for our customers' entire technology stack. Datadog is used by organizations of all sizes and across a wide range of industries to enable digital transformation and cloud migration, drive collaboration among development, operations, security and business teams, accelerate time to market for applications, reduce time to problem resolution, secure applications and infrastructure, understand user behavior and track key business metrics.

Forward-Looking Statements

This press release may include certain “forward-looking statements” within the meaning of Section 27A of the Securities Act of 1933, as amended, or the Securities Act, and Section 21E of the Securities Exchange Act of 1934, as amended including statements on the benefits of new products and features. These forward-looking statements reflect our current views about our plans, intentions, expectations, strategies and prospects, which are based on the information currently available to us and on assumptions we have made. Actual results may differ materially from those described in the forward-looking statements and are subject to a variety of assumptions, uncertainties, risks and factors that are beyond our control, including those risks detailed under the caption “Risk Factors” and elsewhere in our Securities and Exchange Commission filings and reports, including the Quarterly Report on Form 10-Q filed with the Securities and Exchange Commission on February 18, 2026, as well as future filings and reports by us. Except as required by law, we undertake no duty or obligation to update any forward-looking statements contained in this release as a result of new information, future events, changes in expectations or otherwise.

Source: Datadog, Inc.