Datadog's State of DevSecOps 2025 Report Finds Only 18% of Critical Vulnerabilities Are Truly Worth Prioritizing

April 23, 2025 at 4:05 PM EDT

NEW YORK -- Datadog, Inc. (NASDAQ: DDOG), the monitoring and security platform for cloud applications, today released its new report, the *State of DevSecOps 2025*, which found that only a fraction of critical vulnerabilities are truly worth prioritizing.

To better understand the severity of a vulnerability, Datadog developed a prioritization algorithm that factored in runtime context to its Common Vulnerability Scoring System (CVSS) base score. Adding in runtime context provided factors about a vulnerability—for example, whether the vulnerability was running in a production environment, or if the application in which the vulnerability was found was exposed to the internet—that CVSS did not take into account. This helped to reduce noise and identify the issues that are most urgent. After runtime context was applied, Datadog found that only 18% of vulnerabilities with a critical CVSS score—less than one in five—were still considered critical.

"The *State of DevSecOps 2025* report found that security engineers are wasting a lot of time on vulnerabilities that aren't necessarily all that severe," said Andrew Krug, Head of Security Advocacy at Datadog. "The massive amount of noise security teams have to deal with is a major issue because it distracts from prioritizing the really critical vulnerabilities. If defenders are able to spend less time triaging issues, they can reduce their organizations' attack surface all the faster. Focusing on easily exploitable vulnerabilities that are running in production environments for publicly exposed applications will yield the greatest real-world improvements in security posture."

Another key finding from the report was that vulnerabilities are particularly prevalent among Java services, with 44% of applications containing a known-exploited vulnerability. The average number of applications with a known-exploited vulnerability among the other services in the report—Go, Python, .NET, PHP, Ruby and JavaScript—was only 2%.

In addition to being more likely to contain high-impact vulnerabilities, Java applications are also patched more slowly than those from other programming ecosystems. The report found that applications from the Java-based Apache Maven ecosystem took 62 days on average for library fixes, compared to 46 days for those in the .NET-based ecosystem and 19 days for applications built using npm packages, which are JavaScript-based.

Other key findings from the report include:

- **Attackers continue to target the software supply chain**: Datadog's report identified thousands of malicious PyPI and npm libraries—some of these packages were malicious by nature and attempted to mimic a legitimate package (for instance, passports-js mimicking the legitimate passport library), a technique known as typosquatting. Others were active takeovers of popular, legitimate dependencies (such as Ultralytics, Solana web3.js, and lottie-player). These techniques are used both by state-sponsored actors and cybercriminals.
- **Credential management is improving, but slowly**: One of the most common causes of data breaches is long-lived credentials. Last year, 63% of organizations used a form of long-lived credential at least once to authenticate GitHub Actions pipelines. This year, that number dropped to 58%, a positive sign that organizations are slowly improving their credential management processes.
- **Outdated libraries are a challenge for all developers**: Across all programming languages, dependencies are months behind their latest major update. And those that are less frequently deployed are more likely to be using out-of-date libraries—dependencies in services that are deployed less than once a month are 47% more outdated than those deployed daily. This is an issue for developers as outdated libraries can increase the likelihood that a dependency contains unpatched, exploitable vulnerabilities.

For the report, Datadog analyzed tens of thousands of applications and container images within thousands of cloud environments in order to assess the types of risks defenders need to be aware of and what practices they can adopt to improve their security posture.

Datadog's *State of DevSecOps 2025* is available now. For the full results, please visit: https://www.datadoghq.com/state-of-devsecops/. To learn how Datadog helps companies secure their cloud environments, visit: https://www.datadoghq.com/product/cloud-security-management/.

About Datadog

Datadog is the 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 Annual Report on Form 10-K filed with the Securities and Exchange Commission on February 20, 2025, 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.

Contact
Dan Haggerty
press@datadoghq.com