SYNOPSYS®

NGINX Open Source

Helping developers ensure code quality and security with Coverity Scan

Company overview

One of the world's most widely used web servers—powering sites such as Netflix, Hulu, Pinterest, and GitHub—NGINX Open Source (pronounced "engine x") is known for its high performance, stability, rich feature set, simple configuration, and low resource consumption. Other members of the NGINX Open Source family include NGINX JavaScript (njs), a module adding JavaScript support to NGINX; and NGINX Unit, a dynamic application server supporting applications written in Perl, Python, Ruby, Node.js, Go, Java, and PHP.njs.

Developers for all three NGINX Open Source projects use Coverity Scan® to find and fix defects in their code. A free online service provided by Synopsys and powered by the same engine used by Synopsys' commercial Coverity static analysis tool, Scan helps open source developers identify code defects for fast and easy remediation.

"I have a strong belief in the power of open source," said Igor Sysoev, the software's author and cofounder of NGINX in a 2014 interview. "NGINX was an experiment focused on a very specific problem—how to handle more customers on a single, existing server. It turned out to be a universal problem. As soon as I realized NGINX really helps to improve web performance, I wanted people to use it, so I made it open source."

A web server that can also be used as a reverse proxy, load balancer, mail proxy, and HTTP cache, the open source version of NGINX powers more than 400 million websites, including brands such as Netflix, Hulu, Pinterest, and GitHub. Sysoev cofounded NGINX in 2011 to provide formal support for NGINX Open Source and to offer a commercial version, NGINX Plus, which adds enterprise-grade features to NGINX Open Source.

NGINX was acquired by F5 Networks, an application security and delivery company, in 2019. Today, the NGINX family of open source projects include njs, a module adding JavaScript support to NGINX and NGINX Unit, a dynamic application server.

The problem: Ensuring open source code quality and security

"We integrated Coverity Scan into our CI/CD pipeline soon after establishing NGINX," said Maxim Konovalov, one of the company's cofounders and now VP of engineering. "We've been submitting NGINX build artifacts daily since 2012."

"In many cases, NGINX acts as an internet front end," continued Konovalov. "Its security and stability are essential to its users. My team is passionate about code quality and are always looking for best practices and tools to help us improve it. Static code analyzers such as Coverity Scan provide a great help to us."

NGINX takes its role as a foundational technology to millions of apps and websites very seriously. Code quality and security are part of its ethos, and the tools that help support that mission are integral to its development practices.

The solution: Static code analysis with Coverity Scan

Contrary to popular opinion, most software vulnerabilities are the result of coding mistakes, not malicious attacks. According to the "2020 State of the Octoverse" security report, 83% of the vulnerabilities that GitHub sent alerts on from 2019 through 2020 were due to coding errors rather than malicious intent.

But malicious attacks **do** exploit flaws in code, and developers need to embrace proactive detection tools to uncover bugs in the code they write. Static analysis examines source code against a set of coding rules to uncover common coding errors. A free service for open source developers who have registered their projects with scan.coverity.com, Coverity Scan is powered by the same engine used by Synopsys' commercial Coverity static analysis tool to help open source developers identify code defects for fast and easy remediation. A 2020 report from the Linux Foundation surveying open source contributors noted that respondents "overwhelmingly cited Coverity Scan and Clang security checkers" as the primary static analysis tools they use.

The results: 658,000 lines of code scanned with a defect density of 0.02%

In the January 2021 Coverity Scan of a NGINX build, 658,665 lines of code were analyzed, and various code defects uncovered, including two CWE Top 25 defects. Thanks to F5's regular use of Coverity Scan, the NGINX project has a defect density (number of defects per 1,000 lines of code) of only 0.02%.

"Coverity Scan provides an invaluable service to us," says Maxim Konovalov. "I regularly recommend Coverity Scan and its ability to provide specific defect IDs in code commits. And in fact, I'm a member of the FreeBSD committers group, and we use Coverity Scan for code analyses of FreeBSD as well."

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com