Visuality Systems

Continual Code Improvement with Coverity SAST

Company overview

Headquartered in Yokneam, Israel, Visuality Systems Ltd. is the leading global developer and provider of server message block (SMB) protocol solutions, a data and printer communication protocol providing shared access to files and printers across nodes on a network. With a client list of over 150 market-leading companies, Visuality Systems provides the most comprehensive Microsoft SMB client and SMB server solutions, which are used in a variety of embedded products, Java-based applications, and storage systems.

The challenge: Rigorous testing of code quality and security

"Software security is a priority to our customers and something they expect from trusted partners such as Visuality," said Limor Segal-Shevah, automation manager at Visuality Systems. "We wanted to clearly demonstrate that our solutions have been rigorously tested to protect our customer's products and applications."

A leader in developing SMB client and server-based solutions, Visuality's client roster includes industry leaders in consumer devices, aerospace and defense, automotive, and industrial and medical devices. Visuality's NQ product line is the most common commercial SMB solution used in the world today.

"Whether printers, home appliances, Java applications, medical equipment, or automotive entertainment systems, our customers create a variety of software applications running on different hardware and software, each with specific requirements," said Segal-Shevah.

"All have the need for network connectivity because in today's world, devices and applications can't work in isolation anymore. Many applications and embedded devices are communicating with back-end Windows systems through the server message block or SMB protocol, the default standard in Windows systems. Network vulnerabilities can provide hackers with the opportunity to gain access to confidential information or use a system to execute attacks," Segal-Shevah said.

"Software vulnerabilities are usually the result of coding mistakes," she continued. "Malicious attacks exploit flaws in code, and Visuality developers need proactive detection tools to uncover bugs in the code they write to avoid those flaws."

The solution: Coverity Static Analysis

Already using Black Duck Defensics® Fuzzing to identity defects in running code, Visuality added Black Duck Coverity® Static Analysis in 2019 to help its development teams address coding defects early in the software development life cycle. Coverity is a fast, accurate, and highly scalable static analysis solution that helps development and security teams address security and quality defects and ensure compliance with security and coding standards.

Coverity lets Visuality developers scan their code for security weaknesses and quality defects without disrupting their normal workflow. Developers using Coverity can determine the speed and depth of their analyses by choosing between fast desktop, incremental, or full analysis modes. Fast desktop and incremental analyses can help developers find flaws as they code—where they are easiest to find and cheapest to fix. Coverity's full analysis mode integrates with build/CI tools and fails the build if flaws violate a security or quality policy. DevOps teams have the control to manage their

"Coverity is a powerful tool that helps Visuality Systems continually improve our product and ultimately write better and secured code."

analyses depending on their changing needs.

"Coverity is integrated into our CI/CD process," said Segal-Shevah. "We use Bitbucket and Jira Cloud for our software teams to manage their workflow and dynamically show information about new issues discovered in pull-request build. Coverity is integrated into the build process through Python and Jenkins CI. Every piece of code written is checked by Coverity and can't be merged into the main branch of development until passed by Coverity. When a bug is first detected, the responsible developer receives notification of the failure in Slack bot, fixes the problem, and then pushes the code to the cloud, which triggers a new pull request build. The cycle repeats until we have successful results."

The results: Better code, higher customer satisfaction

"We've seen improvements in both the quality and stability of our code," noted Segal-Shevah. "Rather than a customer finding an issue and our going back-and-forth with them to solve the problem, we're resolving code issues in-house before the software ships. The bottom line is that customers receive better code."

"From my perspective, what I like best about Coverity is having comprehensive information and the ability to filter that information for such things as priorities, risk, and individual developer owners. I can filter for only the new issues that were discovered in the latest build. I have the ability to set whatever I want in the filters, which is great. We use the filtering feature constantly, as well as the notification feature whenever something in the database has changed."

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.