GrammaTech Introduces Software Supply Chain Security Platform

CodeSentry Uses Binary Analysis to Create Software Bill of Materials, Detect Zero-Day and N-Day Vulnerabilities and Provide Risk Scoring for Third Party Software Applications

BETHESDA, Maryland/Offenburg, Germany, 6 July 2021

GrammaTech, a leading provider of application security testing products and software research services, today announced the latest version of CodeSentry which reduces software supply chain security risks like those exploited in recent attacks on downstream users of SolarWinds, CodeCov and other applications. CodeSentry quickly analyzes purchased or commercial off the shelf software to identify application components, generate a software bill of materials (SBOM) and detect zero-day and N-day vulnerabilities.

"Most organizations go to great lengths to ensure the safety and security of their physical supply chains yet do very little to assess the integrity of the code used to run their business. Recent incidents like the SolarWinds attack have shined a light on software risk and its consequences," said Mike Dager, CEO of GrammaTech. "CodeSentry enables organizations to discover what components are in the software they are building or using, detect the presence of potential vulnerabilities and mitigate risk. CodeSentry also automates compliance with the SBOM requirement detailed in the recent Executive Order on Cybersecurity."

CodeSentry Binary Analysis

Organizations have traditionally trusted software vendors to manage security risk associated with the applications they purchase. But the increasing frequency of software supply chain attacks is forcing enterprises to proactively assess and verify third party software for vulnerabilities that expose them to threats. Since source code is rarely available for purchased applications, binary analysis is the only alternative for extracting a SBOM to detect underlying risks in commercial software products. Derived

from research conducted for defense and intelligence agencies, CodeSentry provides the following capabilities and benefits:

- *Creates Comprehensive SBOM* – binary scanning identifies open source and third-party components and provides security score, component match details, version information, location, and detailed vulnerability information including CVSS scores
- *Zero- and N-Day vulnerability detection* – detects unknown (zero-day) and known (n-day) vulnerabilities in identified open source and third-party components
- *Executive Dashboard* – provides a software application risk score based on detected vulnerabilities, CVSS and key performance indicators (KPIs)
- *Advanced reporting* - for compliance and risk governance audits
- *Multiple SBOM formats* – including industry standard CycloneDX
- *Flexible deployment* – native SaaS application with optional on-premises deployment

"The increasing reliance by application developers on open source and third party components is a big reason why the software supply chain is vulnerable to being exploited by attackers," said Chris Rommel, Executive Vice President for VDC Research. "Consequently, both application providers and end-user organizations need visibility into the code bases they sell and use so they can continually prove software integrity and proactively detect and mitigate vulnerabilities."

Top Use Cases

CodeSentry addresses the following challenges facing both software providers and enterprises:
IT Vendor Risk Management – reduce risk to the enterprise by assessing the components and security of commercial of the shelf software (COTS) applications such as financial, HR, video conferencing, messaging and other productivity applications.
Information Security – ensure a strong security posture by proactively testing COTS applications for vulnerabilities before rolling them out departmentally or across the enterprise.
DevSecOps – secure the third party code that is brought into the software development life cycle to assure it has been designed and architected with security across the entire stack.

Availability

GrammaTech CodeSentry 2.0 is available immediately from GrammaTech and its German business partner Verifysoft Technology GmbH www.verifysoft.com

About GrammaTech

GrammaTech is a leading global provider of application security testing (AST) solutions used by the world's most security conscious organizations to detect, measure, analyze and resolve vulnerabilities for software they develop or use. The company is also a trusted cybersecurity and artificial intelligence research partner for the nation's civil, defense, and intelligence agencies. GrammaTech has corporate headquarters in Bethesda MD, a Research and Development Center in Ithaca NY, and publishes Shift Left Academy, an educational resource for software developers.

Visit GrammaTech at https://www.grammatech.com/ or have a look to Verifysoft's CodeSentry webpage: https://verifysoft.com/en_grammatech_codesentry.html