

CodeSentry 4.1: Sicherheitslücken in der Softwareentwicklung erkennen

Neue Version der Binärcode-Analyseplattform von GrammaTech identifiziert Risiken im Code von Drittanbietern auch ohne Zugriff auf den Quellcode

Bethesda, USA / Offenburg, 25. November 2022

GrammaTech (<http://www.grammatech.com/>), ein führender Anbieter von Lösungen für die Analyse und das Testen der Softwaresicherheit, hat die neue Version 4.1 seiner Plattform CodeSentry vorgestellt. Als Binärcode-Analysetool erhöht CodeSentry die Sicherheit innerhalb der Software-Lieferkette und ermöglicht es Unternehmen, Sicherheitsschwachstellen im Code von Drittanbietern zu erkennen. CodeSentry setzt dabei auf die Analyse der Softwarezusammensetzung (Binary Software Composition Analysis / BSCA). Dadurch lassen sich bekannte Bedrohungen (CVE) sowie Schwachstellen (Common Weakness Enumeration / CWE) in extern entwickelten Softwarekomponenten auch ohne Zugriff auf den Quellcode identifizieren.

In der neuen Version 4.1 können mehr als 4.700 neue Sicherheitslücken von CodeSentry gemeldet werden. Weiter verbessert wurde die Komponentenerkennung für PE- und COFF-Binaries, ebenso wie die Unterstützung zur Javascript-Package-Detection bei Vorhandensein von package-lock.json- oder yarn.lock-Dateien. Das Analysetool bietet jetzt außerdem eine noch höhere Genauigkeit bei der Versionserkennung von Open-Source-Komponenten in DLLs. Interessant für den Einsatz im behördlichen Umfeld ist die Möglichkeit, CodeSentry in der Version 4.1 nun auch in AWS GovClouds auszuführen. Im Zuge des Updates wurden darüber hinaus mehrere Open-Source-Komponenten von Drittanbietern aktualisiert.

„Software-Entwicklungsteams stehen zunehmend vor der Aufgabe, die Integrität ihrer Produkte zu gewährleisten, indem sie Sicherheitsmängel vermeiden, die zu kostspieligen Ausfällen oder Rückrufen führen können“, erklärt Mike Dager, CEO von GrammaTech. „Dieses Sicherheitsbedürfnis hat inzwischen sogar dazu geführt, dass öffentliche Stellen wie die US-amerikanische Lebensmittelüberwachungs- und Arzneimittelbehörde FDA gesetzliche Anforderungen an die Software-Lieferkette gestellt haben. CodeSentry 4.0 ermöglicht es Unternehmen und Organisationen, den Inhalt und die Sicherheit der Softwarekomponenten von Drittanbietern, die sie zur Erstellung ihrer Produkte verwenden, eingehend zu analysieren und zu überprüfen.“

Während mit Initiativen wie der Open Source Security Foundation (OpenSSF) häufig vor allem Schwachstellen in Open Source Software im Fokus stehen, bleibt ein ebenso wichtiges Problem bestehen. Nach Angaben von VDC Research enthalten fast 60 % aller Softwareprodukte Code von Drittanbietern, wobei „unter der Haube“ meist Open-Source-Komponenten verwendet werden. Da dieser vorgefertigte Code im Binärformat geliefert wird, sind Unternehmen nicht in der Lage, darin enthaltene Sicherheitsrisiken zu erkennen, bevor sie ihn zur Entwicklung von Anwendungen oder zur Einbettung in Produkte wie medizinische Geräte, Fahrzeuge usw. verwenden.

CodeSentry 4.1 bietet umfassende Unterstützung für Desktop- und mobile Anwendungen, Firmware, Container und eingebettete Betriebssysteme, um Schwachstellen in Drittanbieter- oder vorgefertigtem Code während des Entwicklungsprozesses zu erkennen. Die Lösung wird als SaaS- oder On-Premises-Lösung angeboten und bietet eine breite Abdeckung binärer SCA-Plattformen:

- Desktop, Server und mobile Plattformen: Windows, Linux, macOS, Java, Android und iOS
- Sprachunterstützung: Python, JavaScript und Binärdateien aus C/C++, C#, Java und Go
- Eingebettete Betriebssysteme: VxWorks, QNX, Android
- CPU-Architekturen: x86, ARM32/64, MIPS und AVR32
- Dateiformate: Eingebettete und Firmware-Dateisystem-Image-Formate, mobile Dateiformate, Docker-Container sowie Python- und Javascript-Pakete
- Unterstützung mehrerer SBOM-Formate, einschließlich SPDX und CycloneDX

Verfügbarkeit

CodeSentry ist ein Produkt des US-amerikanischen Unternehmens GrammaTech. Vertrieb und Support erfolgen im deutschsprachigen Raum über die Verifysoft Technology GmbH. Kostenfreie Evaluationen sind über www.grammatech.com und www.verifysoft.com erhältlich.

Über GrammaTech

GrammaTechs Softwarelösungen versetzen Firmen in die Lage, sicherere Software zu entwickeln, indem Sicherheitslücken, Software-Bugs und andere Schwachstellen aufgedeckt werden. Dies verringert die Fehlerrate und die Wahrscheinlichkeit für erfolgreiche Cyber-Attacken. GrammaTech CodeSentry ist in DevSecOps-Workflows integrierbar, um Bugs und Sicherheitslücken in Quellcode und Drittanbietercode aufzudecken. GrammaTech engagiert sich darüber hinaus in der Forschung für Software-Sicherheit und ist wichtiger Partner von bedeutenden amerikanischen Institutionen wie DoD, DARPA und NASA. GrammaTech hat seinen Hauptsitz in Bethesda (Maryland) und verfügt über ein Forschungs- und Entwicklungszentrum in Ithaca (New York).

Über Verifysoft Technology

Die Verifysoft Technology GmbH ist ein führender Anbieter von Tools, Dienstleistungen und Schulungen zur Steigerung der Softwarequalität. Die 2003 gegründete Firma betreut über 700 Kunden in 41 Ländern. Schwerpunkt von Verifysoft ist die Messung der Code Coverage (Testüberdeckung) und der Codequalität. Dazu bietet Verifysoft mit Testwell CTC++, Testwell CMT++ und CMTJava Lösungen an, die in allen sicherheitskritischen Branchen zum Einsatz kommen. Zudem ist Verifysoft Distributor für verschiedene komplementäre Tools zur Qualitätssicherung, wie der Statischen Codeanalyse.

Weitere Informationen zu Verifysoft stehen unter www.verifysoft.com bereit.

Pressekontakt:

FX Kommunikation Felix Hansel / PR-Beratung
Stuhlbergerstr. 3
80999 München
Tel.: +49 89 6230 3490
E-Mail: hansel@fx-kommunikation.de

Firmenkontakt:

Verifysoft Technology GmbH
Technologiepark -In der Spöck 10-12
77656 Offenburg
Tel.: +49 781 127 8118-0
E-Mail: quality@verifysoft.com

CodeSonar und CodeSentry sind eingetragene Warenzeichen der GrammaTech, Inc.