GrammaTech veröffentlicht CodeSentry™ zur Identifizierung von Sicherheitslücken in Code von Drittanbietern

Tool zur Analyse der Softwarezusammensetzung erkennt Sicherheitslücken in Anwendungskomponenten und Binärdateien und erstellt eine detaillierte „Software-Stückliste“

BETHESDA, Maryland/Offenburg, Deutschland, 13. Januar 2021 – GrammaTech, ein führender Anbieter von Software-Analyse-Werkzeugen, präsentiert seine neue Lösung CodeSentry. CodeSentry führt eine Analyse der Softwarezusammensetzung (software composition analysis / SCA) durch und inventarisiert Code von Drittanbietern, um darin enthaltene Schwachstellen zu erkennen. CodeSentry identifiziert auf diese Weise mögliche Problemstellen und ermöglicht es Sicherheitsexperten, Risiken während des gesamten Software-Lebenszyklus schnell und einfach abzuschätzen und zu verwalten.

Leistungsfähige Binäranalyse der Komponenten

CodeSentry nutzt eine leistungsfähige Binäranalyse, um eine detaillierte Komponentenliste, auch als Software Bill of Materials (SBOM) bezeichnet, zu erstellen und die dafür bekannten Schwachstellen aufzuzeigen. Drittanbietersoftware kann als Quellcode oder in Binärform verarbeitet werden. Die zugrundeliegenden Komponenten sind der Organisation, die sie verwendet, möglicherweise unbekannt. Es kann sich hierbei um Open Source, Commercial-Off-The-Shelf (COTS) oder Code aus Auftragsentwicklung handeln. CodeSentry ist in der Lage, die damit verbundenen Komponenten und deren Schwachstellen zu erkennen. Dies sind beispielsweise sowohl Netzwerk- und GUI-Komponenten als auch Authentifizierungsebenen.

Spezialisierte Angriffe auf Komponenten von Drittanbietern nehmen zu

Die Notwendigkeit einer solchen Prüfung von Drittanbieterkomponenten wurde in den letzten Jahren durch hochspezialisierte Angriffe immer deutlicher. Diese Attacken zielen darauf ab, bekannte Open-Source-Schwachstellen in Drittanbieterkomponenten auszunutzen. Laut Gartner haben diese Risiken innerhalb der Software-Lieferkette zunehmend an Bedeutung gewonnen. Im Gegensatz zu Schwachstellen, die durch Unachtsamkeit in der Softwareentwicklung entstehen, steigt die Zahl der Fälle, bei denen schädlicher Code mit Absicht von Angreifern in Open-Source-Code eingefügt wird (vgl. Gartner, “Technical Insight for Software Composition Analysis”, November 2019 by Dale Gardner).

„Die Verwendung von Komponenten von Drittanbietern – anstatt diese von Grund auf selbst zu entwickeln – ist gängige Praxis, um die Markteinführungszeit zu verkürzen“, sagt GrammaTech-CEO Mike Dager. „Die meisten Unternehmen stellen mittlerweile jedoch fest, dass Code von Drittanbietern für ihre Anwendungen und ihr Geschäft Sicherheitsrisiken mit sich bringt. Hieraus resultiert die Forderung nach einer Analyse der Softwarezusammensetzung. CodeSentry kann diese Prüfung mit besonderer Präzision durchführen.“

Sicherung des modernen Software-Stacks

CodeSentry basiert auf GrammaTechs bahnbrechender Binär-Code-Analyse und Machine-Learning-Technologie. Das Tool liefert tiefgehende Einsichten in die Software, ohne dass der Quellcode verfügbar sein muss. Weiterhin bietet CodeSentry folgende Hauptvorteile:

- Einfache Nutzung über eine Schnittstelle zum Hochladen von Anwendungen, die native Binärdateien, Zip-Dateien und andere Archive akzeptiert. Für die Binärdateien sind keine Debug-Informationen erforderlich, sie können auf beliebigen Instruction Set Architectures (ISAs) basieren.
- Analyse des tatsächlich auszuführenden Codes anstatt der Build-Umgebung: Durch Weglassen des überflüssigen Codes der Build-Umgebung wird die False-Positive-Rate deutlich gesenkt.
- Identifizierung von Komponenten in nativen Binärdateien durch eine Vielzahl von Algorithmen zur Komponentenvergleichsbestimmung. Erfassung von Versionsnummernbereichen, Erstellung eines Software Bill of Materials (SBOM) mit Links zu CVE und CVSS-Ergebnissen.
- Um ein besonders hohes Niveau der binären Analyse zu erreichen, nutzt CodeSentry mehrere von GrammaTech zum Patent angemeldete Algorithmen. Die spezielle Einbettungstechnologie von GrammaTech ermöglicht es CodeSentry, Komponenten-Disassemblierungen multidimensionalen Vektoren zuzuordnen und diese dann zu vergleichen.

„Kunden, die Software Composition Analysis Tools der ersten Generation nutzen, müssen in der Regel den Nachteil in Kauf nehmen, dass sie keine Einsicht in Softwarekomponenten haben, die als Binärcode geliefert werden“, erklärt Vince Arneja, Chief Product Officer bei GrammaTech. „GrammaTechs Fähigkeit, Binärcode zu analysieren und eine Liste der Softwarezusammensetzung zu erstellen, stellt eine Lösung für Unternehmen dar, die die Angriffsfläche für Hacker proaktiv verkleinern wollen.“

Verfügbarkeit

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

Über GrammaTech

Durch GrammaTechs Softwarelösungen werden Firmen in die Lage versetzt, noch sicherere Software zu entwickeln, indem Sicherheitslücken, Software-Bugs und andere Schwachstellen aufgedeckt und somit die Fehlerrate und die Wahrscheinlichkeit für erfolgreiche Cyber-Attacken verringert werden. Die Tools GrammaTech CodeSonar und CodeSentry sind in DevSecOps-Workflows integrierbar, um Bugs und Sicherheitslücken in Quellcode und Drittanbietercode aufzudecken. GrammaTech ist darüber hinaus in die Forschung für Software-Sicherheit involviert und wichtiger Partner von bedeutenden US-amerikanischen Institutionen wie DoD, DARPA und NASA. Hauptsitz von GrammaTech ist Bethesda (Maryland). Die Forschungs- und Entwicklungsabteilung befindet sich in Ithaca (New York).
Weitere Informationen: www.grammatech.com

Über Verifysoft Technology

Die Verifysoft Technology GmbH ist ein führender Anbieter von Tools, Dienstleistungen und Schulungen zur Steigerung der Softwarequalität und Senkung der Entwicklungskosten im Embedded-Bereich. Das 2003 gegründete Unternehmen betreut mit einem internationalen Beraterteam am Firmensitz in Offenburg über 600 Kunden in weltweit fast 40 Ländern. Ein Schwerpunkt von Verifysoft Technology ist die Messung und Dokumentation der Code Coverage (Testüberdeckung). Dazu bietet Verifysoft Technology mit Testwell CTC++, Testwell CMT++ und Testwell CMTJava Lösungen an, die in allen sicherheitskritischen Branchen zum Einsatz kommen. Zudem ist Verifysoft Technology Distributor für verschiedene weitere Tools zur Qualitätssicherung von Software in Embedded Devices, wie zum Beispiel der Statischen Codeanalyse.
Weitere Informationen: www.verifysoft.com

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: lambertz@verifysoft.com
www.verifysoft.com