Studie: Kommerzielle Softwareanwendungen haben oft kritische Sicherheitsschwachstellen

Sämtliche untersuchten Lösungen enthielten angreifbare Open-Source-Komponenten

BETHESDA, Maryland / Offenburg, Deutschland, 11.11.2021 – GrammaTech, ein führender Anbieter von Tools zur Absicherung der Software-Anwendungssicherheit, hat die Ergebnisse einer gemeinsam mit Osterman Research durchgeführten Studie zum Stand der Sicherheit in Software-Lieferketten veröffentlicht. Der Bericht ergab, dass 100 % der getesteten kommerziellen Standardanwendungen (commercial off-the-shelf/COTS) Open-Source-Komponenten mit Sicherheitsschwachstellen enthielten. 85 % davon waren kritisch.

Von den am häufigsten getesteten Browser-, E-Mail-, Dateifreigabe-/Cloud-Speicher-, Online-Meeting- und Messaging-Produkten enthielten 85 % mindestens eine kritische Schwachstelle mit einem CVSS-Wert (Common Vulnerability Scoring System) von 10,0 – dem höchstmöglichen Wert. Gleichzeitig enthielten 30 % aller Open-Source-Komponenten aller getesteten Anwendungen mindestens eine Schwachstelle oder Sicherheitslücke, die mit einer CVE-Kennung (Common Vulnerabilities and Exposures) versehen war.

„Kommerzielle Standard-Softwarelösungen enthalten oft Open-Source-Komponenten. Viele davon weisen eine Reihe von bekannten Schwachstellen auf, die von Malware ausgenutzt werden können. Doch die Anbieter geben deren Vorhandensein oft nicht bekannt“, sagt Michael Sampson, Senior Analyst bei Osterman Research. „Dieser Mangel an Transparenz rund um eingesetzte und noch einzusetzende Anwendungen ist im Grunde eine Zeitbombe, die das Sicherheitsrisiko eines Unternehmens, die Angriffsfläche und das Potenzial für eine Kompromittierung durch Cyberkriminelle erhöht.“

Im Rahmen der Studie wurden weit verbreitete, clientbasierte COTS-Softwareprodukte in fünf Kategorien (Webbrowser, E-Mail, Dateifreigabe/Cloud-Speicher, Online-Meetings und Messaging) daraufhin untersucht, ob sie Open-Source-Komponenten enthalten und ob sie Sicherheitslücken aufweisen.

Einige der wichtigsten Ergebnisse waren:

- **Lösungen für Online-Meetings und E-Mail am anfälligsten**
  Anwendungen in den Kategorien Online-Meetings sowie E-Mail-Clients wiesen die höchste durchschnittliche Gewichtung der Schwachstellen auf. Angesichts der weit verbreiteten Nutzung dieser Tools sollten Unternehmen und Organisationen den Fokus darauf richten, ihre Angriffsfläche für Sicherheitsrisiken und das Potenzial für eine Kompromittierung besser zu verstehen.
- **Open-Source-Komponenten sind weit verbreitet**
  Ausnahmslos alle analysierten Anwendungen enthielten Open-Source-Komponenten. Im Durchschnitt enthielten dabei 30 % dieser Open-Source-Komponenten mindestens eine Schwachstelle oder Sicherheitslücke, der eine CVE-Kennung zugewiesen wurde.
- **Komponenten mit kritischen Sicherheitslücken werden häufig verwendet**
  Mit Ausnahme von drei Anwendungen enthielten alle in der Studie untersuchten

Lösungen mindestens eine kritische Schwachstelle mit dem höchstmöglichen CVSS-Wert (10,0). Die nahezu allgegenwärtige Verwendung solcher hochgradig anfälligen Komponenten macht Vergleiche zwischen Anwendungen auf dieser Grundlage bedeutungslos, da alle Anwendungen als anfällig einzustufen sind.

- **Neuere Versionen der Komponenten sind nicht zwangsläufig sicherer**
  Mehrere Komponenten waren in den getesteten Anwendungen in unterschiedlichen Versionen vorhanden. Aber: Neuere Versionen waren dabei nicht immer sicherer, weder gemessen an der Anzahl der verwendeten angreifbaren Komponenten noch hinsichtlich der gewichteten Anzahl der Schwachstellen in jeder Komponente.
- **Komponenten mit den höchsten Risiken**
  Von den Komponenten, die in den analysierten Anwendungen identifiziert wurden, waren zwei Versionen der Open-Source-Komponente von Firefox (nicht der Browser selbst) für 75,8 % aller CVEs verantwortlich. An zweiter Stelle standen 16 Versionen von openssl, die zusammen 9,6 % der CVEs aufwiesen, sowie zwei Versionen von libav, die 8,3 % der CVEs ausmachten.

„Die meisten Unternehmen vertrauen darauf, dass Hersteller ihre Software frei von Mängeln halten. Wie die Analyse zeigt, müssen Unternehmen allerdings ihre eigene Qualitätskontrolle durchführen, um die Sicherheit der gekauften Software zu überprüfen“, sagte Vince Arneja, Chief Product Officer bei GrammaTech. „Die Pflege einer aktuellen Software-Stückliste, in der die Softwarekomponenten und die damit verbundenen Schwachstellen detailliert aufgeführt sind, ist der erste Schritt, um Sicherheitsschwachstellen in kommerziellen Softwareanwendungen sowohl vor als auch nach der Implementierung zu verstehen und zu entschärfen.“

Methodik

Im Rahmen der Analyse setzte GrammaTech seine Lösung CodeSentry ein, um das Vorhandensein von Open-Source-Komponenten in den Binärpaketen der am häufigsten verwendeten Softwareanwendungen zu ermitteln. Die Ausgabeberichte für jede Anwendung wurden Osterman Research im PDF-Format zur Verfügung gestellt.

Weitere Informationen

Der komplette Report kann über folgenden Link bei GrammaTech angefordert werden:
https://codesentry.grammatech.com/wp-form-osterman-research

Die Software CodeSentry, mit der Sicherheitslücken in zugekaufter Software angezeigt werden können, ist in der DACH-Region über die Verifysoft Technology GmbH www.verifysoft.com erhältlich.

Über GrammaTech

GrammaTech ist ein weltweit führender Anbieter von Application Security Testing (AST)-Lösungen, die weltweit von den sicherheitsbewusstesten Unternehmen eingesetzt werden, um Schwachstellen in der von ihnen entwickelten oder verwendeten Software zu erkennen, zu messen, zu analysieren und zu beheben. Das Unternehmen ist außerdem Forschungspartner für Cybersicherheit und künstliche Intelligenz für zivile, militärische und

nachrichtendienstliche Einrichtungen der USA. GrammaTech hat seinen Hauptsitz in Bethesda (Maryland), ein Forschungs-und Entwicklungszentrum in Ithaca (New York). Mit der Shift Left Academy betreibt GrammaTech eine eigene Bildungsabteilung für Softwareentwickler.

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 700 Kunden in 40 Ländern weltweit. Ein Schwerpunkt von Verifysoft Technology ist die Messung und Dokumentation der Code Coverage (Testüberdeckung) und der Codequalität. 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 komplementäre Tools zur Qualitätssicherung von Software, wie der Statischen Codeanalyse.
Weitere Informationen zu Verifysoft Technology 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