

24.04.2025 – 08:59 Uhr

HCLSoftware bringt HCL AppScan API Security auf den Markt

Noida, Indien (ots/PRNewswire) -

Eine umfassende API-Sicherheitslösung, die Unternehmen dabei hilft, ihre API-Ressourcen effektiv zu verwalten und gleichzeitig Risiken zu minimieren.

HCLSoftware, ein weltweit führender Anbieter von Unternehmenssoftwarelösungen, gab heute die Einführung von HCL AppScan API Security in Partnerschaft mit Salt Security bekannt. Dieses umfassende API-Sicherheitsprogramm ermöglicht es Unternehmen, alle ihre API-Ressourcen effektiv zu verwalten und sicherzustellen, dass sie weiterhin einen geschäftlichen Mehrwert liefern, ohne ein erhöhtes Risiko einzugehen.

HCL AppScan API Security wurde entwickelt, um blinde Flecken in der Sicherheit mit einer von Experten geschulten, KI-infundierten Erkennungsplattform zu beseitigen, die alle API-Assets findet und inventarisiert, Unternehmens-API-Standards bei Laufzeit und Entwicklung sicherstellt sowie sich nahtlos in die dynamische Analyse integriert, um Schwachstellen zu erkennen und zu beheben.

Anwendungsprogrammierschnittstellen (APIs) verändern die digitale Landschaft in rasantem Tempo. Mittlerweile entfallen weit über 50 Prozent des gesamten Internetverkehrs auf APIs. APIs erleichtern die nahtlose Kommunikation zwischen Anwendungen und werden heute zur Steuerung von Cloud-Diensten, mobilen Anwendungen sowie Geräten des Internets der Dinge (IoT) eingesetzt. Doch dieser Datenverkehr hat APIs gleichzeitig zu einem führenden Angriffsvektor gemacht, der von böswilligen Akteuren ausgenutzt werden kann, und Unternehmen stehen nun vor einer Reihe neuer Sicherheitsherausforderungen.

„Die wachsende Abhängigkeit von APIs hat dazu geführt, dass robuste API-Sicherheit für unsere Kunden zur Chefsache geworden ist. Sie alle wollen ihre Sicherheitslage verbessern und ihre digitalen Ökosysteme schützen“, sagt Rajesh Iyer, Executive Vice President von HCLSoftware.

Im Jahr 2023 ist sowohl die Gesamtzahl der API-Angriffe als auch der Prozentsatz der Datenschutzverletzungen im Zusammenhang mit API-Schwachstellen im Vergleich zu den Vorjahren deutlich gestiegen. Und der Trend setzt sich fort. Im jüngsten Bericht „State of API Security 2024“ von Salt Security gaben 37 % der befragten Unternehmen an, einen API-bezogenen Sicherheitsvorfall erlebt zu haben – doppelt so viele wie im Vorjahr. Allein in den ersten sechs Monaten des Jahres 2024 haben verschiedene Nachrichtenagenturen über groß angelegte API-bezogene Angriffe in zahlreichen Branchen berichtet, darunter Social-Media- und File-Sharing-Plattformen, Technologieunternehmen sowie E-Commerce-Websites, um nur einige zu nennen, die zu kompromittierten Daten von Millionen Nutzern führten.

APIs sind inzwischen so allgegenwärtig, dass viele Unternehmen nicht einmal wissen, wie viele sie verwenden. Bei mittleren und größeren Unternehmen kann die Zahl leicht in die Hunderte gehen. APIs spielen heute in jeder Branche eine wichtige Rolle, vor allem bei Funktionen wie Online-Shopping, Medienbereitstellung, Zahlungsgateways, Workflow-Automatisierung, Microservices, Softwareentwicklung – die Liste lässt sich beliebig fortsetzen. Dies bedeutet, dass der erste Schritt zur Sicherung von APIs darin besteht, ein vollständiges und genaues Inventar dessen zu erstellen, was verwendet wird.

„Eine der Schlüsselfunktionen von HCL AppScan API Security ist die Fähigkeit, den gesamten API-Bestand eines Unternehmens kontinuierlich zu erkennen und aufzuzeichnen“, so Colin Bell, CTO von HCL AppScan. „Dies ermöglicht es den Sicherheitsteams, Einblicke in ihre gesamte Sicherheitslage zu gewinnen.“

Der steigende Trend bei API-Angriffen veranlasste das Open Web Application Security Project (OWASP), die OWASP API Security Top 10 zu erstellen – eine Liste der kritischsten Sicherheitsrisiken, die speziell mit APIs zusammenhängen. Die Liste wurde zusammengestellt, um Unternehmen dabei zu helfen, die mit API-Schwachstellen verbundenen Risiken zu verstehen und zu mildern. Dazu gehören Schlüsselbereiche, auf die sich Unternehmen bei der Sicherung ihrer APIs konzentrieren sollten, wie z. B. Broken Object Level Authorization (BOLA), Excessive Data Exposure und Security Misconfiguration, um nur einige zu nennen. Laut dem Bericht „State of API Security 2024“ von Salt Security nutzen 80 % der Angriffsversuche eine oder mehrere der „OWASP API“-Top-10-Methoden, aber nur etwa 58 % der befragten Unternehmen konzentrieren ihre Sicherheitsanstrengungen

auf diese Liste.

„Mit dem Anstieg der API-Sicherheitsvorfälle und der behördlichen Aufsicht müssen Unternehmen eine kontinuierliche Compliance in ihren API-Wirtschaftssystemen aufrechterhalten“, erklärt Michael Nicosia, COO und Mitbegründer von Salt Security. „Durch die Kombination der leistungsstarken Scan-Funktionen von HCL AppScan mit der Echtzeit-Governance von Salt Security und der Sichtbarkeit von Angriffsflächen, einschließlich unserer Erkennung von undokumentierten sowie Schatten-APIs, liefern wir einheitliche Einblicke und eine tiefere Sichtbarkeit über ihre gesamte API-Landschaft. Dies ermöglicht es Unternehmen, Risiken proaktiv zu erkennen und die Einhaltung wichtiger Standards wie PCI DSS, GDPR sowie HIPAA während des gesamten API-Lebenszyklus zu gewährleisten.“

HCL AppScan API Security gewährleistet eine 100-prozentige Abdeckung der OWASP API Security Top 10 Liste und bietet Unternehmen zahlreiche Funktionen für eine robustere API-Sicherheit:

- Reduzierung blinder Flecken in der Sicherheit mit einer von Experten geschulten, KI-gestützten API-Ermittlungsplattform
- Erkennung und Inventarisierung aller APIs, einschließlich Schatten- und Zombie-APIs
- Identifizierung sensibler Daten bei der Übertragung und Gewährleistung der Einhaltung einschlägiger Vorschriften (z. B. DSGVO, HIPAA und PCI DSS)
- Verknüpfung von APIs mit Eigentümern und Funktionen
- Einblicke in die Sicherheitslage Ihrer gesamten API-Landschaft gewinnen
- Sicherstellung von Unternehmens-API-Standards bei Laufzeit und Entwicklung mithilfe von KI-basierten Erkenntnissen, welche die risikoreichsten API-Assets bewerten und priorisieren
- Übernahme branchenüblicher Best Practices mithilfe vorgefertigter Richtlinienvorlagen und einer umfangreichen API-Richtlinienbibliothek
- Integration von API-spezifischen DAST-Schwachstellentests und Verbesserung der Genauigkeit mit aktuellen Spezifikationen, Geschäftslogik sowie API-Konfigurationsdaten

Für weitere Informationen zu HCL AppScan API Security besuchen Sie bitte unsere Website: <https://www.hcl-software.com/appscan>

Informationen zu HCLSoftware

HCLSoftware ist ein weltweit führender Anbieter von Software-Innovationen und die Software-Abteilung von HCLTech. Wir entwickeln, vermarkten, verkaufen und unterstützen transformative Lösungen für verschiedene Branchen, darunter Unternehmen und Industrie, intelligente Abläufe, umfassende Erfahrungen, Daten und Analysen sowie Cybersicherheit. Unser Einsatz für den Erfolg unserer Kundschaft und unsere Kernwerte Integrität, Integration, Wertschöpfung, Mitarbeiterorientierung sowie soziale Verantwortung treiben uns an, erstklassige Softwareprodukte zu liefern, mit denen Unternehmen ihre Ziele erreichen können. Mit einem reichen Erbe an Pioniergeist bedient HCLSoftware mehr als 20 000 Unternehmen, darunter die Mehrheit der Fortune 100 und fast die Hälfte der Fortune 500. Erfahren Sie mehr darüber, wie wir Ihnen helfen können, Ihre Ziele zu erreichen: www.hcl-software.com.

View original content: <https://www.prnewswire.com/news-releases/hclsoftware-bringt-hcl-appscan-api-security-auf-den-markt-302437043.html>

Pressekontakt:

HCLSoftware,
HCLSoftware@bcw-global.com

Diese Meldung kann unter <https://www.presseportal.ch/de/pm/100093161/100930741> abgerufen werden.