



**Parasoft Corp.  
Headquarters**  
101 E. Huntington Drive  
Monrovia, CA 91016  
USA  
[www.parasoft.com](http://www.parasoft.com)  
[info@parasoft.com](mailto:info@parasoft.com)

Pressemitteilung

## **Parasoft: Unterstützung für die brandneuen CWE-Richtlinien des Jahres 2019**

***Mit seinem vollständigen Support und Compliance Reporting für die aktualisierten MITRE-Sicherheitsregeln ist Parasoft der erste Anbieter auf dem Markt***

**Monrovia (USA) / Berlin – 19. November 2019 - Parasoft, führender Anbieter im Bereich des automatisierten Softwaretestings, gibt die umfassende Unterstützung der neu aktualisierten 2019 Common Weakness Enumeration (CWE) Top 25 sowie der „On the Cusp“-Liste (mit weiteren 15 Schwachstellen) für die Sprachen C, C++, Java und .NET bekannt. Mit den neuesten Releases seiner Softwaretest-Produkte Parasoft Jtest, Parasoft dotTEST und Parasoft C/C++test deckt Parasoft als einziger Anbieter alle diese kritischen Security-Richtlinien ab. Damit können Unternehmen durchgehende Sicherheit und Compliance erzielen und die gefährlichsten Softwarefehler abwenden.**

Mit seinen neuesten Releases, welche die neue Generation der 2019 CWE Top 25 unterstützen, kann Parasoft mit lückenlosem CWE-Support aufwarten. Die von Parasoft angebotenen CWE Compliance Packs für C/C++, Java und .NET enthalten vorkonfigurierte, umgehend einsatzbereite und vollständig anpassbare Testkonfigurationen und das Reporting für die Security-Standards CWE Top 25 und CWE CUSP. Die Parasoft-Lösung ist als CWE-kompatibel zertifiziert. Dadurch können die Anwender während der Konfiguration, der Fehlerbehebung und des Reportings einfach erkennen, welcher statische Analysechecker zu welchem Punkt der CWE-Liste gehört. Mit dem spezifischen CWE-orientierten Modell von Parasoft sind sämtliche Checker auf Basis der zugehörigen CWE-ID benannt. Dadurch erübrigt sich ein zeitraubendes Zuordnen beim Konfigurieren, beim Reporting und bei der Problembeseitigung. Das spezielle Echtzeit-Feedback von Parasoft gibt Anwendern kontinuierlichen Einblick auf den Stand der CWE-Konformität,

durch interaktive Compliance-Dashboards, Widgets und Reports, bei denen der CWE Risk Technical Impact direkt im Dashboard implementiert ist.

Wurden die Listen traditionell noch aus den zusammengefassten Ergebnissen von Erhebungen erstellt, die verschiedene Unternehmen über die Häufigkeit und Wichtigkeit von Schwachstellen durchgeführt hatten, beruht die von CWE unlängst angekündigte neue Generation der Top-25- und der „On the Cusp“-Liste auf einem objektiveren, datengetriebenen Prozess, der auf Informationen von Common Vulnerability Enumeration (CVE), NIST und National Vulnerability Database (NVD) zurückgreift. Diese Informationen berücksichtigen den CVSS-Wert (Common Vulnerability Scoring System) einer jeden Schwachstelle oder CVE. Dazu gehören auch Angaben darüber, wie verbreitet eine bestimmte Sicherheitslücke ist, wie schwierig sie von einem Angreifer auszunutzen wäre und welche Auswirkungen die bei einem Exploit auftretenden Schäden haben könnten.

„Die zusätzlichen Informationen aus dem Update von 2019 unterstützen Unternehmen dabei, objektiv zu verstehen, welche Punkte auf der Liste wahrscheinlich den meisten Schaden verursachen werden. Das macht die 2019 CWE Top 25 und die „On the Cusp“-Liste für das Thema Cybersecurity effektiver“, erläutert Arthur Hicken, Security-Experte bei Parasoft. „Die Nutzung eines SAST-Tools, das beide Listen vollumfänglich abdeckt, hilft sicherzustellen, dass die Software den maximal möglichen Grad an Sicherheit bietet. Der lückenlose CWE-Support und das leistungsstarke Reporting- und Analysesystem von Parasoft unterstützen unsere Kunden dabei, nicht nur Sicherheitslücken vor dem Release aufzuspüren, sondern sich um die ermittelten Grundursachen der Security-Probleme zu kümmern und den Code so besser zu schützen.“

Die durchgängigen Testlösungen von Parasoft für C/C++, Java und .NET bieten unerreicht breite Unterstützung für die Security-Standards CWE Top 25 und „On the Cusp“. Das spezielle, auf CWE ausgerichtete Modell von Parasoft erlaubt es den Anwendern ferner, die Ergebnisse der statischen Analyse mit jenen von CWE zu verknüpfen, ohne dass wie bei anderen Tools mühsame Zuordnungen oder zusätzliche Arbeit erforderlich sind.

**CWE** ist eine umfassende Liste mit mehr als 800 Programmier-, Design- und Architekturfehlern, die zu ausnutzbaren Schwachstellen führen können. Zuletzt im Jahr 2011 aktualisiert, liegt mit den „2019 CWE Top 25 Most Dangerous Software Errors“ nunmehr eine gekürzte Liste mit den am weitesten verbreiteten und gefährlichsten Fehlern vor, die bei Ausnutzung zu schwer wiegenden Folgen für die Sicherheit der Software führen können. Seit ihrem Erscheinen ist die Top-25-Liste in einer Vielzahl von Branchen zu einem verbreitet angewandten Sicherheitsstandard geworden – gemeinsam mit der etwas weniger bekannten „On the Cusp“-Liste der CWE. Für Unternehmen, die das Thema Cybersecurity ernst nehmen, bilden diese weiteren 15 Punkte den nächsten Schritt in Sachen AppSec, wenn die Top 25 vollständig unter Kontrolle sind. Für Teams, die mit IoT oder Medizingeräten zu tun haben, sind die Top 25 und die „On the Cusp“-Liste zudem ein integraler Bestandteil der UL-2900-Konformität, die auch die FDA anerkennt.

Details zur Unterstützung von Parasoft für die CWE Top 25 und die ‚On the Cusp‘ Regeln stehen unter

<https://www.parasoft.com/solutions/compliance/cwe>.

# # #

**Über Parasoft ([www.parasoft.com](http://www.parasoft.com)) :**

Parasoft liefert innovative Tools, die zeitaufwändige Tests automatisieren und dem Management die intelligente Analytik für die Konzentration auf das Wesentliche zur Verfügung stellen. Die Technologien von Parasoft verringern den Zeit-, Arbeits- und Kostenaufwand für die Ablieferung sicherer, zuverlässiger und konformer Software durch die Integration von statischer Analyse und Laufzeit-Analyse, Modul-, Funktions- und API-Tests und Service-Virtualisierung. Parasoft unterstützt Software-Unternehmen bei der Entwicklung und dem Deployment von Applikationen auf dem Embedded-, Enterprise- und IoT-Markt. Mit seinen Testwerkzeugen für Entwickler, seinen Report- und Analyse-Werkzeugen für Manager und seinen Dashboard-Lösungen für Führungskräfte gibt Parasoft Organisationen die Möglichkeit, die strategisch wichtigsten Entwicklungs-Initiativen von heute (Agile, Continuous Testing, DevOps und Security) erfolgreich umzusetzen.

**Pressekontakt:**

Parasoft Corp., Erika Barron, Tel. +1-626-275-2434; erika@parasoft.com  
Agentur Lorenzoni GmbH, Public Relations, [www.lorenzoni.de](http://www.lorenzoni.de)  
Beate Lorenzoni, Tel: +49 8122 55917-22; beate@lorenzoni.de