Parasoft Corp.
Headquarters
101 E. Huntington Drive
Monrovia, CA 91016
USA
www.parasoft.com
info@parasoft.com

Press Release

Parasoft Releases Support for Brand New 2019 CWE Guidelines

Parasoft is first-to-market with full support and compliance reporting for the updated security rule mappings from MITRE

MONROVIA (USA)/Berlin, November 19, 2019 - Parasoft, the global leader in automated software testing, today announced complete support for the newly updated 2019 Common Weakness Enumeration (CWE) Top 25 and "On the Cusp" (an additional 15 weaknesses) for C, C++, Java, and .NET languages. With the latest releases of their software testing products Parasoft Jtest, Parasoft dotTEST, and Parasoft C/C++test, Parasoft is the only vendor to cover all of these critical security guidelines, enabling organizations to achieve continuous security and compliance to prevent the most dangerous of software errors.
Learn more about Parasoft's support for the CWE Top 25 and "On the Cusp" rules here.

The **CWE** is a comprehensive list of over 800 programming errors, design errors, and architectural errors that can lead to exploitable vulnerabilities. Previously updated in 2011, the 2019 CWE Top 25 Most Dangerous Software Errors is a targeted list of the most widespread and critical errors that can be exploited to create the most serious security consequences in software. Since its release, the Top 25 list has been a widely adopted security standard throughout a variety of industries, along with the CWE's somewhat lesser-known "On the Cusp" list. For organizations that are serious about cybersecurity, these additional 15 items are the next step in AppSec, after getting the Top 25 under control. For teams working with IoT or medical devices, both the Top 25 and "On the Cusp" are also an integral part of UL 2900 (Software Cybersecurity for Network-Connectable Products) compliance, recognized by the FDA for network-connected medical device cybersecurity.

Parasoft provides full support for CWE, with its latest releases supporting the new generation of the 2019 CWE Top 25. **Parasoft's CWE Compliance Packs for C/C++, Java, and .NET** provide pre-configured, out-of-the-box, and fully customizable test configurations and reporting for the CWE Top 25 and CWE CUSP security standards. Parasoft's solution is certified CWE-Compatible, so users can easily understand which static analysis checker is associated with which CWE item during configuration, remediation, and reporting. With Parasoft's unique CWE-centric model, all the checkers are named based on the associated CWE ID, removing the need for time-consuming mapping when configuring, reporting, and remediating issues. Parasoft's unique real-time feedback gives users a continuous view of compliance with the CWE, by providing interactive compliance dashboards, widgets, and reports that have the CWE risk technical impact implemented right within the dashboard itself.

Having traditionally been constructed through aggregating survey responses from a wide selection of organizations on weaknesses considered to be the most prevalent or important, CWE's recently-announced new generation of the Top 25 and "On the Cusp" lists have used a more objective data-driven process that leverages information Common Vulnerability Enumeration (CVE), NIST, and from the National Vulnerability Database (NVD). This information takes into account the Common Vulnerability Scoring System (CVSS) score of each vulnerability or CVE, including information about how prevalent a particular vulnerability is, how difficult it might be for an attacker to exploit it, and the impact of the damage they could cause by exploiting it.

"The additional information provided in the 2019 update will help organizations objectively understand which items are likely to cause the most harm, making the 2019 CWE Top 25 and 'On the Cusp' more effective for cybersecurity," explained **Arthur Hicken, security expert at Parasoft**. "Using a SAST tool that covers the entirety of these two lists will help ensure that your software is as secure as possible. Parasoft's complete CWE support and powerful reporting and analytics system helps our customers not only catch security vulnerabilities before they release, but address core root-cause security problems to harden the code."

Parasoft's C/C++, Java, and .NET unified testing solutions provide the broadest support for the CWE Top 25 and "On the Cusp" security standards. Parasoft's unique CWE-centric model provides users with the ability to connect static analysis findings to CWEs without any tedious mapping, or extra effort that is required from other tools.

# # #

About Parasoft:
Parasoft provides innovative tools that automate time-consuming testing tasks and provide management with intelligent analytics necessary to focus on what matters. Parasoft technologies reduce time, effort, and cost of delivering secure, reliable, and compliant software, by integrating static and runtime analysis; unit, functional and API testing; and service virtualization. Parasoft supports software organizations as they develop and deploy applications in the embedded, enterprise and IoT markets. With developer testing tools, manager reporting/analytics and executive dashboarding, Parasoft enables organizations to succeed in today's most strategic development initiatives – agile, continuous testing, DevOps, and security.

Press Contacts:
Parasoft Corp., Erika Barron, Tel. +1-626-275-2434; erika@parasoft.com

Agentur Lorenzoni GmbH, Public Relations, www.lorenzoni.de
Beate Lorenzoni, Tel: +49 8122 55917-22; beate@lorenzoni.de