Engineeringnet techpost

Engineeringnet Mobile

Scan de QR-code of klik hier om mobiel te surfen.

CWI fixt Java-bug met formele methoden

ONDERZOEK & WETENSCHAP 23/02/2015 15:16:57

Onderzoekers van het Nederlandse Centrum Wiskunde & informatica (CWI) hebben in februari 2015 een bug gefixt in de veelgebruikte objectgerichte programmeertaal Java.

ENGINEERINGNET - De bug zat in een veel toegepast sorteeralgoritme, TimSort, waardoor programma's konden crashen.

De fout was al in 2013 bekend maar nog nooit goed opgelost. Toen onderzoeker Stijn de Gouw van de CWI-onderzoeksgroep Formal Methods de correctheid van TimSort wilde bewijzen, stuitte hij op de beveiligingsfout

Hij diende een bug report in met een verbeterde versie. Dat rapport is inmiddels geaccepteerd. Deze versie van TimSort wordt gebruikt door Android.

Het sorteeralgoritme TimSort is onderdeel van de java.util.Arrays en java.util.Collections libraries. Het is genoemd naar de maker, Tim Peters, die het in 2002 ontwierp voor de programmeertaal Python, waar het nu het standaard sorteeralgoritme is.

De sorteerfunctie wordt vaak gebruikt, bijvoorbeeld bij de analyse van data. De Gouw ontdekte dat een eerder voorgestelde fix van de fout niet goed was. Hierdoor kunnen programma's crashen bij een grote invoer die op een bepaalde manier is gesorteerd.

Voor zijn onderzoek gebruikte hij 'KeY', een open source verificatietool, om de mechanische correctheid te bewijzen van TimSort. Daarna ontwierp hij een correctie, met behoud van performance.

Frank de Boer, groepsleider van de Formal Methods groep zegt: "Het was een van de zwaarste bewijzen die tot nu toe zijn uitgevoerd om de correctheid van een bestaande Java-library aan te tonen: het had ruim twee miljoen bewijsregels en duizenden handmatige stappen nodig."

Het onderzoek werd mede-gefinancierd door het EU-project Envisage. << (Guy Leysen) (bron: CWI) (foto: Java)