CWI verhelpt bug in Java met formele methoden

26 FEBRUARI 2015 10:37 | RIK SANDERS

Onderzoekers van het Centrum Wiskunde & informatica (CWI) in Amsterdam hebben een bug gefixt in de veelgebruikte objectgerichte programmeertaal Java. Het gaat om een fout in een veel toegepast sorteeralgoritme, Timsort, waardoor programma's konden crashen. De fout was al in 2013 bekend maar nog nooit goed opgelost. Voor de verbeterde oplossing is de open source verificatietool KeY gebruikt.

Toen onderzoeker Stijn de Gouw van de CWI-onderzoeksgroep Formal Methods de correctheid van Timsort wilde bewijzen, stuitte hij op de fout, die een gevaar kan zijn voor de beveiliging. Hij diende een bug report in met een verbeterde versie. Dat rapport is inmiddels geaccepteerd. Deze versie van Timsort wordt gebruikt door Android.

Java wordt onder meer gebruikt voor serversoftware, internet-gebaseerde bankdiensten en bijvoorbeeld in computerspellen als Minecraft. De programmeertaal wordt zo vaak gebruikt, omdat het veel support biedt in de vorm van bibliotheken (libraries). Zo hoeven ontwikkelaars bijvoorbeeld niet zelf een functie te verzinnen om data te sorteren; die kunnen ze uit de library-support halen.

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.

Niet crashen

Voor zijn onderzoek gebruikte De Gouw KeY, een open source verificatietool, om de mechanische correctheid te bewijzen van Timsort. Daarna ontwierp hij een correctie, met behoud van prestatie (performance). Volgens Frank de Boer, groepsleider van de Formal Methods-groep, is het 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. 'Bij zo'n belangrijke taal als Java is het cruciaal dat software niet crasht. Dit resultaat geeft goed het belang aan van formele methoden voor de maatschappij.'

Het onderzoek werd mede-gefinancierd door het EU-project Envisage. Software is een van de speerpunten van het CWI, waar het onderzoek is uitgevoerd.