

## KORT

## Cees de Visser nieuwe directeur NWO



Cees de Visser mag zich per 1 maart volgend jaar de nieuwe algemeen directeur noemen van de Nederlandse Organisatie voor Wetenschappelijk

Onderzoek (NWO). Tot die datum wordt de organisatie geleid door de huidige ad interim directeur Frank van Eijkern. Op dit moment is De Visser directeur van Nefarma, de koepelorganisatie van alle onderzoeksgeoriënteerde farmaceutische bedrijven in Nederland.

## Energimeter op afstand uitleesbaar

KPN, energieleverancier Oxxio en IBM starten in Nederland met een netwerk voor draadloze, op afstand afleesbare energimeters. De digitale meter stuurt informatie over gas- en elektriciteitsverbruik automatisch door naar een centrale computer. KPN verzorgt de verbindingen in het netwerk en maakt daarbij gebruik van zijn gprs-mobielnetwerk dat speciaal voor draadloze dataoverdracht is ingericht. IBM verzorgt de implementatie en het beheer van het complete systeem.



advertentie

you can  
**Canon**

Zoekt u een efficiëntere manier om informatie vast te leggen, te beheren en te delen?

Dat kan. Bel **0800 - 226 66 84** voor de verkooppunten of kijk op [www.canon.nl/scanners](http://www.canon.nl/scanners).

Papier hier!

# Fouten in C en C++ oorzaak van beveiligingsproblemen

Onderzoek moet programmeur helpen bij vinden veiligheidsrisico's

**Het overgaan van C en C++ naar Java en C# om software minder foutgevoelig te maken, is niet de oplossing voor de risico's die door softwarefouten ontstaan. Programmeurs moeten zich bewust worden van de risico's.**

**S**oftwareprogrammeurs maken te veel fouten. Standaardfouten in de C++-methode liggen aan de wortel van de meeste beveiligingsproblemen. Dat ontwikkelaars zich niet bewust zijn van de problemen, is vooral te wijten aan hiaten in het onderwijsprogramma. Dit zegt Erik Poll, universitair docent softwarebeveiliging aan de Radboud-universiteit in Nijmegen deze week op de pagina's Loopbaan in Computable.

## Geen keus

"Het is goed om te zien dat Erik Poll de noodklok luidt over de veiligheidsrisico's van programmatuur die in C of C++ is ontwikkeld", zegt Arie van Deursen, hoogleraar software engineering aan de Technische

## HERKENBAAR?

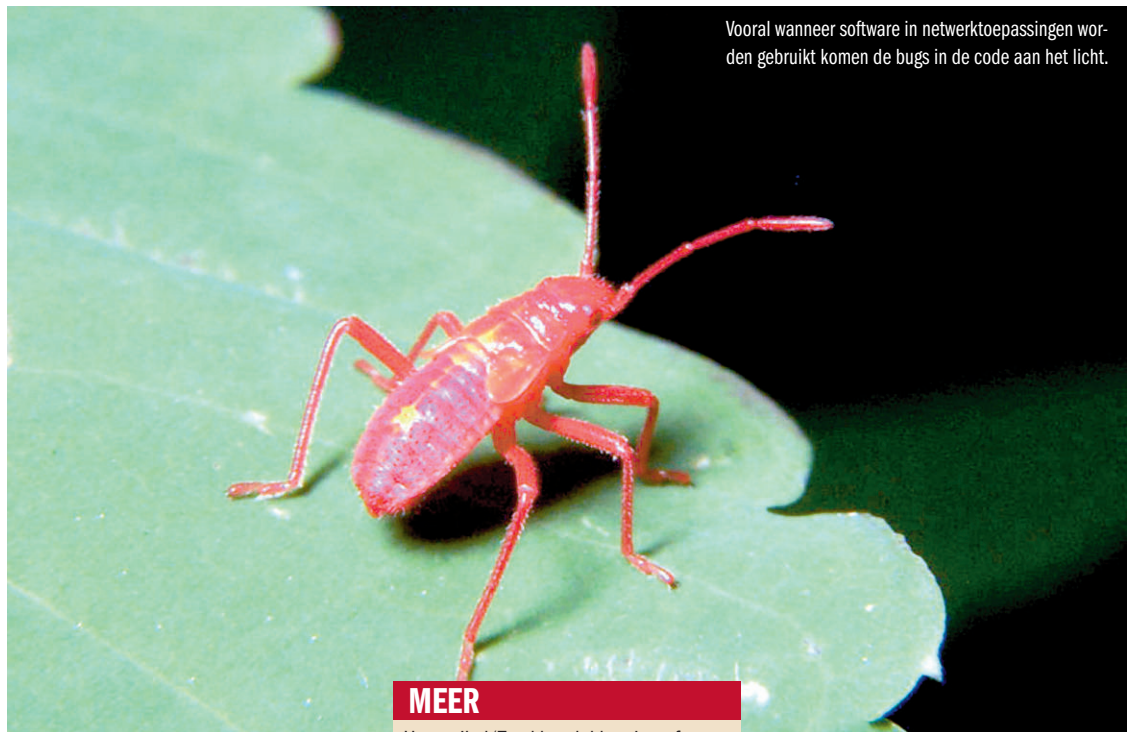
We zijn benieuwd naar uw ervaringen en bevindingen. Komt u veel beveiligingsfouten tegen in C en C++? Moeten daar geen maatregelen voor komen? Wat zou volgens u een passende oplossing kunnen zijn? We lezen uw reactie graag op [computable.lezers@bp.vnu.com](mailto:computable.lezers@bp.vnu.com)!

## REACTIES VAN LEZERS

Het gebruik van de Standard Template Library kan ook al veel problemen i.v.m. geheugenallocaties oplossen en het versnelt het programmeren aanzienlijk.

Jan Boonen

Hoe vaak worden deze misplaatste vergelijkingen niet gemaakt? Een vergelijking tussen C, C++ en Java is alleen zinnig als er iets te vergelijken valt! De taal C is een programmeertaal, terwijl Java een ontwikkelplatform is. Het is hetzelfde om een boekhouder achter zijn geschreven boekhouding te vergelijken met een niet-boekhouder achter een pc



Vooral wanneer software in netwerktoepassingen worden gebruikt komen de bugs in de code aan het licht.

## MEER

Het artikel 'Zwakke plekken in software te voorkomen' kunt u lezen op pagina 35 in dit nummer.

Universiteit van Delft. Toch is de oplossing die Poll schetst, namelijk het overgaan op Java en C#, te kort door de bocht, "want ook in deze talen is het mogelijk om (per ongeluk) een lek in de beveiliging te programmeren", vult collega Leon Moonen, universitair docent aan de TU Delft aan. "Het echte probleem is dat er lang niet altijd een keus is om op een andere programmeertaal over te gaan. Het meeste programmeerwerk wordt gedaan door bestaande systemen aan te passen. De omvang van deze systemen loopt in de honderden miljarden regels code. Hiervan is 10 procent in C geschreven en nog eens 10 procent in C++", aldus Van Deursen. "Om de veiligheidsproblemen die hierdoor ontstaan aan te pakken, is het noodza-

kelijk onderzoek te doen naar programma-analysetechnieken die de programmeur helpen bij het vinden van veiligheidsrisico's, zoals de door Poll genoemde bufferoverflows. Dit onderzoek staat nog in de kinderschoenen, maar is veelbelovend", zegt Moonen. In Delft wordt op dit moment een dergelijk onderzoek uitgevoerd.

## Vanuit de hacker gezien

Ook Kees Hemerik, hoofd van de groep Software Construction aan de Technische Universiteit Eindhoven, herkent het probleem dat Poll schetst. "Veel beveiligingsproblemen

vinden hun oorzaak in het gebruik van de talen C en C++. Die komen pas goed aan het licht wanneer software in netwerktoepassingen wordt gebruikt. Het voorstel om dan maar allemaal in Java of C# te programmeren biedt echter maar weinig soelaas. Deze talen bieden wel meer mogelijkheden voor beveiliging en verificatie, maar ze zijn nog steeds erg complex en omvangrijk." Hemerik bestrijdt dat er in het universitair onderwijs te weinig aandacht wordt besteed aan softwarebeveiliging. "Een mooi voorbeeld is het college 'Hacker's Hut', dat bij ons door professor Andries Brouwer wordt gegeven. In dit college wordt beveiliging vanuit het gezichtspunt van de hacker beschouwd." ■ [KIM LOOHUIS]

met het beste boekhoudprogramma. Je moet wel weten wat je aan het doet bent. En gek misschien, maar ik vertrouw meer op die papieren boekhouder.

Harm Frielink

Het is wel wat naïef om te denken dat alle beveiligingsproblemen zijn opgelost wanneer je C# of Java gaat gebruiken. Maar inderdaad: beide platforms bieden veel meer ondersteuning op het gebied van beveiliging. Als je C++ niet hoeft te gebruiken, dan vooral niet doen. Door Bjarne Stroustrup's starre opstelling is het inmiddels een stoffig taaltje, waar

niet veel ontwikkeling meer in zit. Overigens: C# is niet twee maal zo langzaam als C++. Het scheelt in veel gevallen slechts enkele procenten.

Wim Bokkers

Mijn inziens is het probleem dat kwaadwillenden steeds vaker via de applicatielaag inbreken en dat programmeurs in het verleden kwetsbaarheden hebben verwaarloosd. Slordigheid zou ik hen niet willen verwijten aangezien veiligheid nooit hoog op de prioriteitenlijst heeft gestaan. Ik denk dat de oplossing gezocht moet worden in de combinatie van

bewustzijn en kennis van software-security en technologie die de programmeurs en testers in staat stelt om de code en applicaties op een effectieve en efficiënte manier te valideren op veiligheid. Fortify Software (Palo Alto, California) heeft technologie ontwikkeld om kwetsbaarheden automatisch te detecteren middels Source Code Analyse. De tool vertelt precies in welke coderegel het probleem zit. Door deze technologie krijgen developers een tool in handen waardoor de veiligheid voor hen een beheersbaar probleem wordt.

Jurgen Teulings