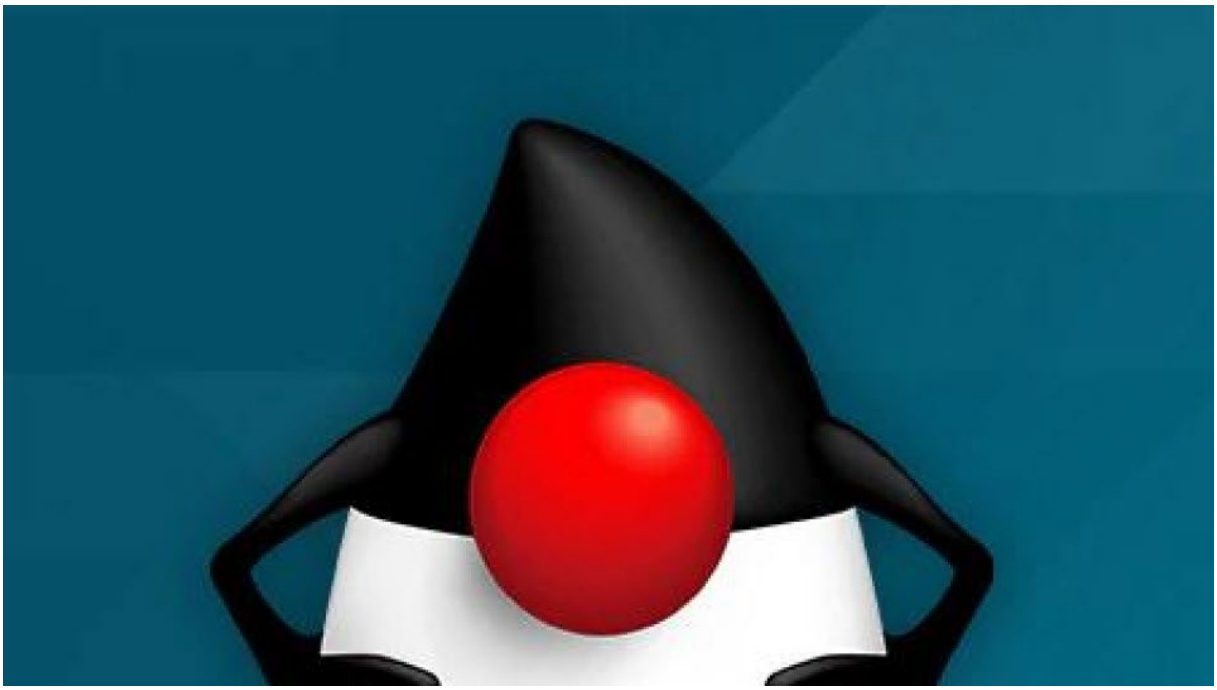
Google beloont Nederlandse ontdekkers van gevaarlijke Java-bug

Onderzoekers aan het Nederlandse techinstituut CWI hebben een bugbounty van Google gekregen voor een belangrijke security-ontdekking in Java. De standaardlibrary LinkedList blijkt een overflow-fout te bevatten die verstrekkende gevolgen kan hebben. Kwaadwillenden zouden dit kunnen misbruiken om onveilige verbindingen te maken met Java-toepassingen.



© Oracle
Oracle

Deze bug is ontdekt toen leden van de CWI-onderzoeksgroep Computer Security de broncode van LinkedList gingen doorspitten. Het doel van dat onderzoek was bewijzen dat die veelgebruikte code geen fouten bevat. Daar zijn de Nederlandse onderzoekers dus niet in geslaagd, omdat ze deze overflow-fout hebben gevonden, merkt CWI-onderzoeker Hans-Dieter Hiep droogjes op.

Verbaasd

Hij uit verbazing dat deze basale bug is aangetroffen in de code voor linked lists, omdat het een goed bekende datastuctuur is die ook wordt onderwezen in informatica-onderwijs én omdat deze Java-library wijdverbreid is qua gebruik. Bovendien is de broncode ervan publiekelijk beschikbaar als open source.

De kwetsbare linked list doet dienst in bepaalde beveiligingsgerelateerde onderdelen van Java, zoals de implementatie van secure sockets in die programmeertaal annex softwareplatform. Secure sockets worden gebruikt voor het bewerkstelligen van beveiligde verbindingen via uiteenlopende internetprotocollen, zoals https, ftps en ssh.

Het CWI (Centrum Wiskunde & Informatica) heeft de ontdekking van de beveiligingsfout gedeeld met de ontwikkelaars van Java, waarna de implementatie van secure sockets is aangepast. Die gebruikt niet langer de linked list met deze fout.

Vroeger geen gevaar

De bug in kwestie schuilt al zo'n twintig jaar in deze Java-software, maar is niet al die tijd ook echt een beveiligingsprobleem geweest. Hiep legt in de CWI-blogpost over de ontdekking uit dat de overflow geheel niet aan de orde was toen de wereld nog 32-bit computers gebruikte. De bug kon niet 'geactiveerd' worden simpelweg omdat er niet genoeg geheugenruimte was. De overstap naar 64-bit processors heeft computers echter veel meer geheugenruimte gegeven, waardoor deze overflow dus een concrete kwetsbaarheid is geworden.