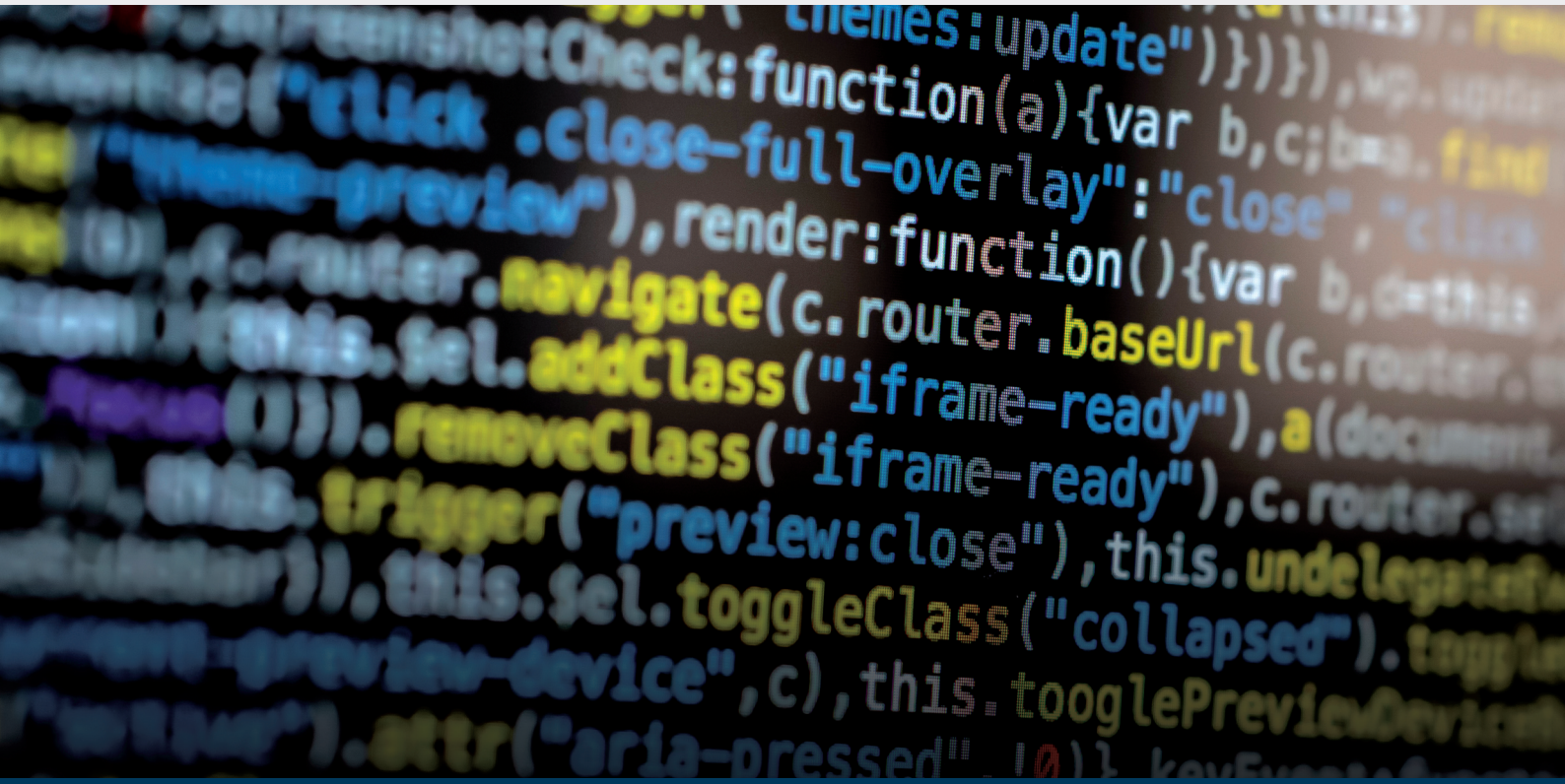
In deze rubriek geven enkele iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.



Log4shell - een cadeau voor de maatschappij aan het einde van 2021?

Log4shell is een referentie naar een kwetsbaarheid in een Java class Log4j. De wereld werd op 10 december 2021 verrast door het bekend worden van deze kwetsbaarheid, terwijl dit al eerder ontdekt was. Velen dachten: "We hebben wel meer kwetsbaarheden in onze infrastructuur, wat is het probleem?"

Er bestaat een unauthenticated remote code execution kwetsbaarheid in de populaire Java-library 'Apache Log4j 2'. Deze library wordt door veel op Java gebaseerde toepassingen gebruikt voor logging doeleinden. Door de kwetsbaarheid kan een aanvaller een willekeurige code uitvoeren binnen het Java-proces. In het Financieel Dagblad werd dit vergeleken met suiker. Het zit in allerlei producten, soms zonder je medeweten (1). Door deze kwetsbaarheid zijn alle organisaties alert gemaakt van het belang van cybersecurity. Is dit een mooi cadeau of niet?


Chris de Vries


Fook Hwa Tan


Maarten Hartsuijker

Patching is belangrijk, maar niet altijd even makkelijk – Fook Hwa Tan

Het waren drukke dagen voor de kerst, toen veel organisaties hun infrastructuren moesten inventariseren om na te gaan of deze java-library aanwezig was. Velen begonnen in te zien hoe belangrijk het kennen van je eigen IT-omgeving wel niet is. Je kunt niet controleren wat je niet weet. Uitdaging bij deze kwetsbaarheid was ook, dat het niet altijd duidelijk was of de software gebruik maakte van deze java-library. Het was een race tegen de klok om zowel van buiten als van binnen je netwerk af te speuren naar het gebruik van deze programmatuur.

Vervolgens werd je geconfronteerd met het feit dat oudere software mogelijk niet zo kwetsbaar was en dat het slechts om specifieke versies ging. Er kwamen discussies op gang over wat het nut ervan was om deze oude versies te updaten, omdat je nu niet kwetsbaar zou zijn. Soms werd dit zelfs aangedragen als bewijs, dat actueel houden van software soms misschien ook slecht is voor je beveiliging. Neemt niet weg dat in oudere versies van deze software er natuurlijk ook nog andere kwetsbaarheden zaten die je zou willen patchen.

Als laatste verrassing kwam men er na een aantal dagen achter dat de patch ook nog kwetsbaar was en er inmiddels ook weer een nieuwe versie beschikbaar werd gesteld. Wil je na een hectische week patchen, nogmaals alle systemen patchen? Patchen is belangrijk, maar last minute van alles moeten bijwerken is vaak geen doen!

Nog lang last van Log4j – Maarten Hartsuijker

Log4Shell heeft ons allemaal weer even gewezen. En hoewel dat goed is voor ons 'veiligheidsbewustzijn', is een lek als dit natuurlijk een verschrikking. Gelukkig kwamen er snel patches en workarounds beschikbaar. Maar waar deze kwetsbaarheid zich enorm in onderscheidt van de andere kwetsbaarheden, is zijn complexiteit. Daar waar misbruik ervan uitblonk in eenvoud, is het voor veel organisaties verschrikkelijk moeilijk om in te schatten wáár ze precies kwetsbaar voor zijn.
Waar je een belangrijke Windows of Linux update over het algemeen met één druk op de knop doorvoert, moet je er bij Log4j eerst erachter komen of de module ergens verstopt zit. Als je eigen development teams hebt die software bouwen, kunnen de teams dit veelal bij software die nog actief in ontwikkeling is wel snel inschatten. Maar neem je applicaties of software af van derden, dan is dit al veel lastiger. Is log4j aanwezig? Bevat de laatste firmware ook de patch? Deze informatie wordt door leveranciers vaak niet actief noch in detail gedeeld. En als berichten de keten in gaan en ergens diep in het netwerk een applicatie raken van een log4j module erin, dan is het ook eenvoudig om de kwetsbaarheid over het hoofd te zien óf in te schatten wat de impact van de kwetsbaarheid is. We gaan van dit lek nog heel erg lang last hebben.

Bewustworden, bewustzijn en onvermogen – Chris de Vries

Soms ligt het antwoord zo voor de hand en schrijf je 1-2-3 de waarheid op. Dan begin je te twijfelen, verlangzaam je het denken en ga je op zoek naar wijsheid. Ik wil er op zo'n moment weleens een etymologisch of een groot woordenboek der Nederlandse taal op naslaan. Zo ook hier:

- bewustworden: het proces van betekenis toekennen aan gebeurtenissen in de praktijk;
- bewustzijn: het vermogen tot besef, tot weten en erkennen van jezelf en van de dingen;
- onvermogen: de machteloosheid om ondanks het bewustzijn de situatie aan te passen!

En wat heeft dit nu te maken met het Log4j hoor ik u denken? Veel. In december (van vorig jaar) hoorden wij van deze grote dreiging. Ik werd erop geattendeerd door een relatie en vele anderen vernamen het via het nieuws. Ah … het proces van bewustworden!
Vervolgens het besef dat de dingen niet zijn zoals ze horen te zijn (de gevaren) en de start van het zoeken naar oplossingen (`patches' of hardware aanpassingen). Bingo … het bewustzijn naar vermogen te acteren of te laten acteren! En drie: de oplossing implementeren. Eh… welke? Nee toch, sta ik opeens voor mijn onvermogen? Dat hield in mijn geval in dat ik niet in staat bleek om alle mogelijke kwetsbaarheden op te sporen en dat na raadpleging van mijn systeembeheerder het meest effectieve was om mijn iDrac-kabel los te koppelen en aanvullende 'back-ups' te draaien. Conclusie: zo leidt 'awareness' niet altijd tot preventie. Wederom blijkt dat het MKB vaak niet in staat is zelf de dreiging te keren en professionals – naar beste eer en geweten – kunnen trachten dat op te lossen, maar dat evenmin kunnen garanderen. Wat nu…? Een soort klimaatverandering die wij maar lijdzaam hebben te ondergaan? Oftewel spreken wij hier over een 'total system hack', niet te verwarren met de 'total recall' film!

Referentie

(1) https://fd.nl/tech-en-innovatie/1423175/nationale-cyberwaakhond-roept-beveiligers-bijeen-vanwege-wereldwijd-lek-xca2cawKb9w0