Vragen m.b.t. Memo Java kwetsbaarheid log4j – Update januari 2022

Partij	Nr.	Vraag / Input	Antwoord / Reactie
GroenLinks	1	U schrijft dat u de specifieke applicaties en systemen die in de organisatie in gebruik zijn, en die vanwege de kwetsbaarheid risico lopen, heeft geïnventariseerd en zult nagaan of deze kwetsbaarheid inmiddels is afgewend of deze software nog veilig kan worden ingezet. Is voor alle applicaties en systemen inmiddels helder hoe het ervoor staat (kwetsbaarheid gepareerd en software veilig)? En voor zover dat nog niet helder is, kunt u aangeven welke gevolgen een inbreuk op de systemen waarvan dit nog niet helder is zou hebben? Heeft u in kaart welke gegevens in dat geval risico op misbruik lopen en in welke risico klasse die vallen?	Alle bij PU bekende applicaties/systemen zijn vooralsnog veilig. Het is onzeker of er in de kwetsbare periode backdoors in de systemen van leveranciers geplaatst zijn door kwaadwillenden. Daardoor blijft het mogelijk dat er in de toekomst alsnog incidenten kunnen ontstaan veroorzaakt door Java kwetsbaarheden Log4J. Met onze IT-leveranciers (netwerk en servers) houden we nauw contact. Zij zijn ook in de CERT-procedure opgenomen, zodat er snel geschakeld kan worden indien noodzakelijk. Het devies blijft “verhoogde dijkbewaking”. Ook is het de intentie om een scan te laten uitvoeren op alle bij PU bekende internet-facing ip-adressen en URL’s van IT-dienstenleveranciers van PU. Dit is een weerbarstig proces omdat alle leveranciers informatie moeten aanleveren om zo’n scan mogelijk te maken. De systemen die opgenomen zijn in het BCM (BedrijfsContinuïteit Plan) krijgen extra aandacht m.b.t. beschikbaarheid, integriteit en vertrouwelijkheid.