Príomhoifigeach Faisnéise

Oifig an Phríomhoifigeach Faisnéise,
FSS, Ospidéal Dr Steevens,
Baile Átha Cliath 8, D08 W2A8

Chief Information Officer

Office of the Chief Information Officer,
HSE, Dr. Steevens' Hospital, Dublin
8, D08 W2A8

www.hse.ie
ehealthireland.ie
@hselive
t 01 635 2732

28th January 2022

Mr. Alan Kelly TD
Dáil Eireann
Leinster House
Dublin 2

Re: PQ re 2237/22

''To ask the Minister for Health if the HSE has put a plan in place to deal with vulnerabilities in its computer networks (details supplied); if so, the details of same; the action that has been taken; the person who is leading the plan; when the HSE first responded to the issue; when the HSE first become aware of the issue; the meetings that were held to resolve the issue; the steps his Department has taken; and if he will make a statement on the matter.'' (Log4j vulnerabilities in its computer networks)

Dear Deputy Kelly,

The HSE were made aware of the significance of the log4j vulnerability at 16:49 on 10th December.

Log4j is a tool to help the programmer output log statements to a variety of output targets. It is normally used in case of problems with an application, it is helpful to enable logging so that the problem can be located. The log4j package is designed so that log statements can remain in shipped code without incurring a high performance cost. It follows that the speed of logging (or rather not logging) is capital.

At the same time, log output can be so voluminous that it quickly becomes overwhelming. One of the distinctive features of log4j is the notion of hierarchical loggers. Using loggers it is possible to selectively control which log statements are output at arbitrary granularity.

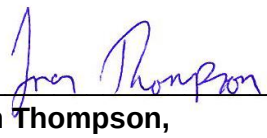
The HSE were made aware of the significance of the log4j vulnerability at 16:49 on 10th December.

This was immediately communicated across all security areas including security partners. Following detailed consultation with security and system partners, and wider communication across the Health IT community, appropriate detection and remediation recommendations were applied over the following days.

There are some residual activity ongoing with respect to applications with medium term remediation plans which are managed under the governance of ICT. There are mitigating controls in place, which with the support of cyber security partners, will stop any known Log4j vulnerabilities at a network level. These controls have been in place since 11th December 2021.

If you feel that the question has not been fully answered or you require any further clarity, please contact me.

Yours sincerely,



Fran Thompson,
Interim Chief Information Officer, OoCIO, HSE.