Yukon
Information
and Privacy
Commissioner

3162 Third Avenue, Main Floor
Whitehorse, Yukon, Y1A 1G3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.yukonombudsman.ca

Advisory for custodians and public bodies regarding the Log4j vulnerability

December 21, 2021

Audience

This advisory is intended for anyone with responsibility for the operation or content of IT systems containing personal health information (PHI) or personal information (PI) including custodians[1] under Yukon's *Health Information Privacy and Management Act* (HIPMA) and public bodies[2] under Yukon's *Access to Information and Protection of Privacy Act* (ATIPPA).

Overview

On December 10, the Apache Software Foundation released an advisory[3] regarding a critical remote code execution vulnerability in Log4j. Log4j is a logging utility[4] written in the Java programming language. Log4j is widely used in software and is one of the most popular logging modules used by applications written in Java. In turn, Java is one of the most popular programming languages in use and many applications may consequently rely in some way on Log4j.[5] Reporting indicates that, as a result of this vulnerability, exploitation, data theft and ransomware attacks have been observed.

Purpose

This advisory is issued to inform custodians and public bodies about the risk of the Log4j vulnerability and about actions that can be taken to mitigate the risk of a breach of PHI or PI that could occur as a result of the vulnerability.

[1] Custodians are defined under HIPMA and include but are not limited to doctors, dentists, pharmacists, optometrists, physiotherapists, chiropractors and operators of health care facilities.

[2] See the schedule of the ATIPPA regulation for a list of public bodies here.

[3] https://logging.apache.org/log4j/2.x/security.html

[4] This type of logging utility provides diagnostic information to software developers regarding the performance (or lack thereof) of the software.

[5] Java is often used for the back end of websites, in case or electronic (medical) record systems or in reporting components of applications.

Details for management of the Log4j vulnerability

- PHI or PI in your organization may be at risk of unauthorized access, theft, or of becoming unavailable.
- Under both HIPMA and ATIPPA, you as a custodian or public body have an obligation to adequately protect PHI or PI that you hold.
- You must ensure that your information technology (IT) service provider or IT department (systems service provider) assesses your IT systems for the use of software that may rely directly or indirectly on the Log4j vulnerability.
- Because there is a risk of a breach of privacy from this vulnerability, we recommend that, at minimum, your systems service provider ensures that:
  - public facing (directly internet exposed) systems that are vulnerable are investigated for signs of breach;
  - public facing (directly internet exposed) systems that are vulnerable are immediately patched;
  - barring the ability to immediately patch, these systems are confined to your internal network;[6]
  - any systems on the internal network are patched as soon as possible; and
  - if software used is vulnerable to Log4j and cannot be patched (e.g. no vendor support) and no workaround is available, the software should be retired or the data (PHI/PI) migrated to adequately protected systems, and, while these steps are being taken, the system running the vulnerable software must be sufficiently isolated to minimize the risk of breach as a result of the vulnerability.
- There may be additional measures that your systems service provider should take depending on your IT systems and storage of PHI or PI.

General information about the vulnerability for IT

- Log4j is a Java library used in many products and frameworks including Apache Struts2, Apache Solr, Apache Druid, Apache Flink and Apache Swift. Other Java frameworks also include it in their libraries, including but not limited to: Netty, MyBatis and the Spring Framework. Also see CVE-2021-44228.[7]
- Versions of Log4j between 2.0-beta9 to 2.16 are vulnerable. The initial patch that was released has flaws so the latest patches available should be used. See CVE-2021-45046[8] and CVE-2021-45105[9].

[6] A pre-condition here is that your internal network is reasonably secure and has basic security controls, including proper access controls, in place.

[7] https://nvd.nist.gov/vuln/detail/CVE-2021-44228

[8] https://nvd.nist.gov/vuln/detail/CVE-2021-45046

[9] https://nvd.nist.gov/vuln/detail/CVE-2021-45105

- The vulnerability allows a remote unauthenticated actor to execute arbitrary code on an affected device.
- While the highest risk is for public facing systems, there is significant risk for internal systems too.
  - Insider threats or compromised systems that can interface with vulnerable internal systems will be able to exploit the vulnerability on these systems.
  - Logging may be triggered by unexpected events. This may in some scenarios allow this vulnerability to be triggered without needing direct access to any interface but through intermediary systems.

Future developments

It is anticipated that the ways in which this vulnerability can be leveraged will develop over time. Given this, we recommend that systems service providers for custodians and public bodies keep a close eye on news about this vulnerability including information released by NIST[10], CISA[11], and CCCS[12] for the latest developments regarding critical vulnerabilities.

Obligation to report privacy breaches

Both custodians and public bodies are required to notify individuals about a breach of their PHI or PI where there is a risk of significant harm to the individuals as a result of the breach. In addition, Yukon's Information and Privacy Commissioner (IPC) must be informed about the breach.

Should a breach of privacy occur as a result of the Log4j vulnerability, custodians and public bodies need to assess whether they are required to notify individuals about the breach and inform the IPC. Failure to notify individuals and the IPC about a breach as required is an offence under both HIPMA and ATIPPA.

Contact information for Yukon Information and Privacy Commissioner

Call (867) 667-8468 (tollfree in Yukon 1-800-661-0408 ext 8468). Email info@yukonombudsman.ca

Disclaimer

The purpose of this document is to inform custodians and public bodies about the risks to privacy associated with a recent information security development and to support them in meeting their privacy and security obligations under HIPMA and ATIPPA.

This document is not intended as, nor is it a substitute for legal advice or advice about how to secure or protect PHI or PI that may be at risk of breach as a result of the information security development. This document is not binding on Yukon's Information and Privacy Commissioner.

[10] https://nvd.nist.gov/vuln
[11] https://www.cisa.gov/uscert/
[12] https://cyber.gc.ca/en/alerts-advisories