CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

What is Log4j and Why Did the Government of Canada Turn Everything Off?

by Alexander Rudolph

January 2022

POLICY PERSPECTIVE

WHAT IS LOG4J AND WHY DID THE GOVERNMENT OF CANADA TURN EVERYTHING OFF?

by Alexander Rudolph

January 2022

The author wishes to give special thanks to Rachel Babins of Emerging Leaders in Canadian Security for assistance in writing this article.

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1800, 150 – 9th Avenue S.W., Calgary, AB T2P 3H9
www.cgai.ca

ISBN: 978-1-77397-224-4

On December 10, 2021, the Canadian Centre for Cyber Security (CCCS) issued a security advisory regarding a critical vulnerability and called for users and network administrators to make the needed changes and updates to mitigate the threat. The vulnerability is in Apache Log4j, a widely used open-source tool for logging and recording activity in specific software applications and online services. The Log4j tool is so ubiquitous that some media are writing headlines such as "The Internet is on Fire." Many industry insiders describe the vulnerability as among the worst in a decade, and have given it a severity score of 10/10.

So how bad is it, really? So bad that Quebec shut down almost 4,000 websites – just as a precaution. Even the federal government is not immune to the potential threat. The Canada Revenue Agency and Public Services and Procurement Canada, among others, have systematically taken down service infrastructure that might be affected, as a precautionary measure. But how bad can vulnerability in a logging application be?

How Bad is Bad and How Does it Affect Canadian National Security?

This vulnerability, called a remote code execution (RCE), allows individuals who are not authorized to remotely run code and commands on an affected system. Specifically, the vulnerability in Log4j can allow an untrusted, unauthorized user to take over a server by telling it to download or execute malicious code without the server's owner being aware. Why? Because the same logging tool that would tell you this happened is used to conduct the attack.[1] What the Log4j vulnerability and many RCE vulnerabilities do is to provide an entry point for would-be attackers to run malicious code on a remote device. The threat is not the Log4j vulnerability itself but how threat actors can use it for malicious purposes. Think of this security vulnerability as akin to a heavily guarded government facility whose fence is no longer impenetrable due to a sinkhole. Whether it's a criminal looking for a ransom or a malicious actor looking to harm Canadians, it is a vector of attack for unsavoury elements.

Fixing the issue is not always as easy as applying a patch. The Apache Software Foundation, the non-profit which maintains Log4j, released an emergency patch to fix the vulnerability, but for stability reasons it may not be an option for some people. With the release of any patch comes the risk of inadvertently breaking other features, slowing down the application or unknowingly creating new vulnerabilities. In addition to just how widespread this is, what makes the Log4j vulnerability so severe is the ease with which it can be exploited. One of the first instances of its exploitation was in the popular video game Minecraft.[2] Attackers were able to copy and paste malicious code into the chat box that all players can access. While this may seem initially trivial, this vulnerability can be used to infect the Minecraft servers with any code the attackers want to

[1] While there are other methods of catching this exploitation, the threat actor's ability to hide their actions from the recording tool itself is among the reasons this vulnerability is so severe.
[2] Minecraft is one of the best-selling games ever and had as many as 126 million players a month in April 2020.

accomplish their goal, including ransomware.[3] It took less than a week for ransomware groups to take advantage of this vulnerability and infect Minecraft servers and players alike. By Christmas, the criminals taking advantage of this vulnerability had expanded to include some of the largest and most sophisticated ransomware groups.

So surely, we can isolate the affected servers, patch them, and we'll be safe? While mitigation measures exist to help identify and alert administrators when a system or network has been compromised, they are not panaceas. The challenge is determining which systems are affected. Log4j is built upon the Java programming language, which was used by approximately 90 per cent of Fortune 500 companies in some capacity, according to a 2018 analysis. Because of how ubiquitous Log4j and Java are across networks and software development, security software company Sophos recommends that network administrators find all software and applications on a system that uses Java to check if it has the Log4j vulnerability. Tools have already been developed to search for such code quickly and easily, but these tools do not work on all systems.

Fortunately, the Canadian government and large corporations are readily equipped to address and mitigate the threat. In addition, many federal and provincial websites and systems are maintained by third-party IT service providers with greater experience, knowledge and assets to respond to such emergencies quickly. Complicating things further, however, such third-party IT service providers are often themselves vulnerable to large supply chain weaknesses. Many municipalities and small and medium-sized businesses that may not have in-house or managed IT services may be unaware that they are vulnerable. Still, despite greater resources, the November attack on Newfoundland and Labrador's health-care system highlights that even provinces with managed IT services are vulnerable. The lesson is that complacency is not an option, but this assumes that all parties are aware that they are vulnerable in the first place and actively working to stop and mitigate such threats.

So, what about people and organizations who are unaware they are vulnerable? CrowdStrike, an industry-leading cyber-security firm, found in their 2021 Global Security Attitude Survey that 66 per cent of respondents said their organizations had experienced a ransomware attack in the previous 12 months. Thus, a wide-ranging software vulnerability like Log4j moves from being a cyber-security issue to a national security issue because the private sector and regular Canadians will be affected the most.

Software Vulnerabilities as National Security Threats

When federal and provincial governments begin to take down websites, this is not a sign of being unprepared. Rather, it is a positive step towards patching or mitigation. Patching and fixing the issue may be the quickest solution, but it is not always the perfect option. Further, depending on the system, patches may not even be possible. In such a case, mitigation is necessary to prevent vulnerability to exploitation in the first place. In the best-case scenario, settings can be modified

[3] Ransomware is a type of malware that is designed to encrypt a victim's personal data and block access unless the victim pays a ransom. It is often accompanied by threats to leak the victim's data unless payment is promptly made.

to deny actors the ability to exploit the vulnerability. In a slightly worse case, the entire logging tool has to be replaced, which is easier said than done. In the worst-case scenario, a threat actor has infected your system and moved across your network to infect other computers. The precarious position thus created prolongs the state of insecurity as long as the vulnerability remains unfixed. This is the situation security professionals in information technology face daily, and not just for the Log4j vulnerability.

The CCCS, Canada's leading organization to address cyber-security, knows of at least 235 ransomware incidents against Canadians between January 1 and November 16, 2021. However, it may be impossible to know the full number because some companies keep it a secret to avoid extra costs associated with bad publicity or punishment for not having sufficient security, which affects business beyond the ransomware attack. These facts and figures also predominantly overlook the human factor. Canadians who have been individually affected by such attacks are unlikely to report that they were victims. CCCS assesses that ransomware payments have stabilized at approximately $200,000, but the recovery process can be much more than the payment itself. The global average recovery cost from a ransomware attack is approximately $2.3 million. CCCS notes that more than half of ransomware victims in the first half of 2021 were in the critical infrastructure sector, which includes energy, health and manufacturing. Behind each of these ransomware attacks is a vulnerability, whether something like Log4j, a weak password, badly set network policies or an untrained user who opens an infected email attachment. On December 14, 2021, Superior Plus disclosed that it was the target of a ransomware incident. Superior Plus, a distributor of propane and related products, servicing 780,000 clients in the United States and Canada, has taken the affected systems offline but told reporters that production was not affected.

This type of incident is no longer making headlines because of how common it's becoming; that is, unless it rises to the level of the Colonial Pipeline attack. The Colonial Pipeline ransomware attack targeted the U.S.'s largest fuel pipeline in 2021, causing panic and gas shortages. The attack led President Joe Biden to declare a state of emergency and sign an executive order to strengthen U.S. cyber-defence. These efforts have largely been applauded, but debate remains about the executive order's effectiveness. Regardless, national security policy cannot be developed on an ad hoc basis from crisis to crisis. Cyber-threats are highly evolving and fast-moving and addressing their impacts requires a proactive process on behalf of the public and private sectors.

Vulnerability Disclosure and Mitigation as National Security Practice

Just as violence is endemic to the international system, vulnerability is endemic to cyber-space. The Canadian government is proactively protecting the state by passing laws and prosecuting criminals who use cyber-space. The government has developed an offensive capability in the Communications Security Establishment (CSE), given the Canadian Armed Forces a mandate to develop offensive cyber-capabilities (albeit with questionable results), and more. The CSE recently revealed that it conducted an offensive cyber-operation against ransomware operators, the first time it publicly admitted to doing so. News of this action was followed days later by reports that the Ontario Provincial Police arrested a Canadian man who was charged with

ransomware attacks. As much as these mechanisms and capabilities help to address insecurity, once the vulnerability is known and disclosed, mitigation must be done universally and "in the wild."[4] However, is this enough to address the effects of the current threat environment?

Addressing the sources of insecurity is among the best approaches to secure cyber-space, but once a vulnerability is known, there is no putting it away. In most cases, we do not hear about or feel the effects of vulnerabilities because they are found by researchers, hackers and software developers who then disclose the vulnerability to the affected parties. Under perfect circumstances, these vulnerabilities are caught and disclosed through formal disclosure programs before malicious actors can exploit the flaw. Under less-than-ideal circumstances, malicious actors have already begun to exploit the vulnerability before the developers are aware of it or can patch it. In either scenario, the CCCS plays a crucial role by providing alerts on critical vulnerabilities found and advisories on how to mitigate by patch or other method. Further, in either case, once a vulnerability has been disclosed, it has the dual effect of warning people to patch or take action to protect themselves, and it tells malicious actors about the vulnerability. The Log4j vulnerability is this last example taken to the most critical levels of cyber-infrastructure and has affected nearly everyone, which is why there is a pressing need for other government departments and ministries to act. In the United States, the Federal Trade Commission warned corporations they may face legal action, like the $700 million fine for the Equifax data breach, because corporations have a "duty to take reasonable steps to mitigate software vulnerabilities" and must patch or mitigate the Log4j vulnerability. Indeed, warnings of punitive actions are a strong motivator, and the Government of Canada should be looking at how to incentivize improving cybersecurity.

CyberSecure Canada

CyberSecure Canada is an initiative launched by Innovation, Science and Economic Development Canada and is an example for the rest of government. It is a cyber-security certification program for small and medium-sized organizations to encourage them to protect themselves from cyber-threats. For some organizations, this will be an easy process as their exposure to cyber-threats is limited, but many others will be surprised to learn just how vulnerable they are. Fundamentally, understanding enough to know you are not equipped to address such threats and should consult with experts is a positive step to becoming secure, for knowing is half the battle. Indeed, CyberSecure Canada is a positive step, but it does not go far enough to encourage the private sector to secure itself.

This certification program can, and should, be taken further to provide direct competitive or economic benefits for organizations. The program and certification currently provide non-tangible economic benefits under the promise that it will help reduce the risk of cyber-threats and provide a competitive advantage in the marketplace. The first of these two goals is a near certainty.

[4] "In the wild" refers to when a vulnerability is known to those who intend to use it for malicious purposes, often said when the vulnerability is already being exploited by threats.

By becoming certified, your business will be better protected and reduce the risk of a cyber-incident if the protections are followed. The second of the two remains to be seen. The program should be lauded as it is a great step towards increasing baseline cyber-security standards throughout Canada. However, its legitimacy and efficacy as a certification will only come with time and has yet to be proven a competitive advantage. The program's promised advantages cannot be quantified easily, and any benefits from it would be in the longer term. The rewards as presented are vague at best.

On December 6, 2021, the ministers of National Defence, Public Safety, Emergency Preparedness and International Trade co-signed an open letter to Canadian organizations about ransomware. They warned Canadians about increasing cyber-threats, particularly ransomware, and advised them that following basic cyber-security best practices can prevent the majority of incidents. Indeed, top levels of the federal government are aware of the issue and are elevating it to make people and organizations aware that they must protect themselves. However, the statement highlights the need to move beyond awareness campaigns.

To increase the direct economic advantages of enhancing security, a CyberSecure Canada certification should be a requirement for federal procurement. As CyberSecure Canada was only launched recently, it would not be smart to make it mandatory immediately. Nevertheless, Public Services and Procurement Canada must develop a timeline to phase in this requirement, or add it to current contracts. It would be to the benefit of bidders, the government of Canada and Canadians alike. Similarly, the Canadian government should look towards greater co-operation with industry, particularly in information security and offensive security, to develop a business case for policies which can increase the economic and financial advantages of improved cyber-security. The need for greater government-industry collaboration on cyber-security and cyber-defence is not new, but is something the Canadian Association for Defence and Security Industries (CADSI) has long stressed is necessary. In particular, CADSI called for the creation of a government-industry forum to address systemic issues associated with the federal procurement of cyber.

Ensuring Canada's cyber-security and cyber-defence is not something a single minister or certification program can do. This is recognized in part by the current government as the new mandate letters tasked the Ministers of National Defence, Foreign Affairs, Public Safety and Industry, Science and Development to develop a new National Cyber Security Strategy. Each minister must consider how their mandate can be used to decrease the costs associated with adopting improved cyber-security practices and increasing incentives to undertake the process. However, it is an error to assume that these ministers have sole responsibility over Canadian cybersecurity. Being cyber-secure is not something one can achieve, but is rather a reiterative process. And with digital connectivity in nearly every facet of daily life, relegating security to government authorities runs counter to how we interact with the internet. The government can – and has – put resources in place to help enhance security in cyber-space and has made great strides in developing awareness of the issue. Now it needs to incentivize the adoption of a proactive stance towards vulnerabilities and threats, which would have encouraged the prompt and effective handling of the Log4j vulnerability.

Resources

Have you or your organization been targeted in a malicious cyber-incident? You can report it to the CCCS on their website. The CCCS also has a learning hub, which provides learning activities, programs and courses that cost only what was incurred for delivery of the courses. Get Cyber Safe is Canada's national public awareness campaign, which contains easy tutorials and information about how Canadians and organizations can better protect themselves.

About the Author

Alexander Rudolph *is a Ph.D. Candidate in the Department of Political Science at Carleton University. Alex's research explores grand strategy, conflict, and competition in cyberspace. As part of his research in comparative cyber defence policy, Alex incorporates sociology, information security, and open source intelligence methods to research the strategic thought and doctrine of cyber conflict and how it informs the creation of cyber force structures.*

Outside of his academic work, Alex is an American-Canadian ex-pat and regularly contributes to Canadian and international discussions on cyber conflict. Alex has more than 10 years of experience working for non-profits in the public education and advocacy sectors as a project manager and analyst. Presently, Alex is Vice-President of Emerging Leaders in Canadian Security, a non-profit dedicated to supporting young and new professionals in Canadian security and defence, and works in Ottawa as a research coordinator in defence consulting.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.