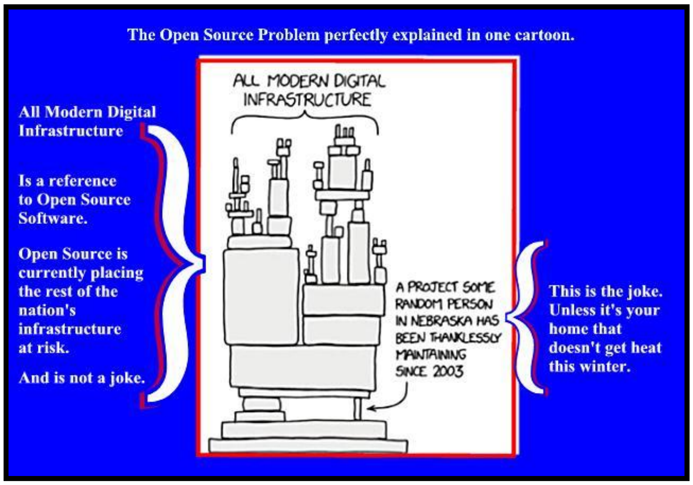
Top

Back to Contents
A Printable PDF of this post is available here.

The Next Looming Supply Chain Crisis,
Or, Open Source Chickens Come Home To Roost

Remember this?


The Open Source Problem perfectly explained in one cartoon.
All Modern Digital Infrastructure
Is a reference to Open Source Software.
Open Source is currently placing the rest of the nation's infrastructure at risk.
And is not a joke.
ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003
This is the joke. Unless it's your home that doesn't get heat this winter.

The problems of open source software have been known for some time. Yet, open source is and continues to be the foundation upon which the Internet works. Paradigms do shift, though. And our global conflict is forcing a reevaluation of our reliance on open source software.

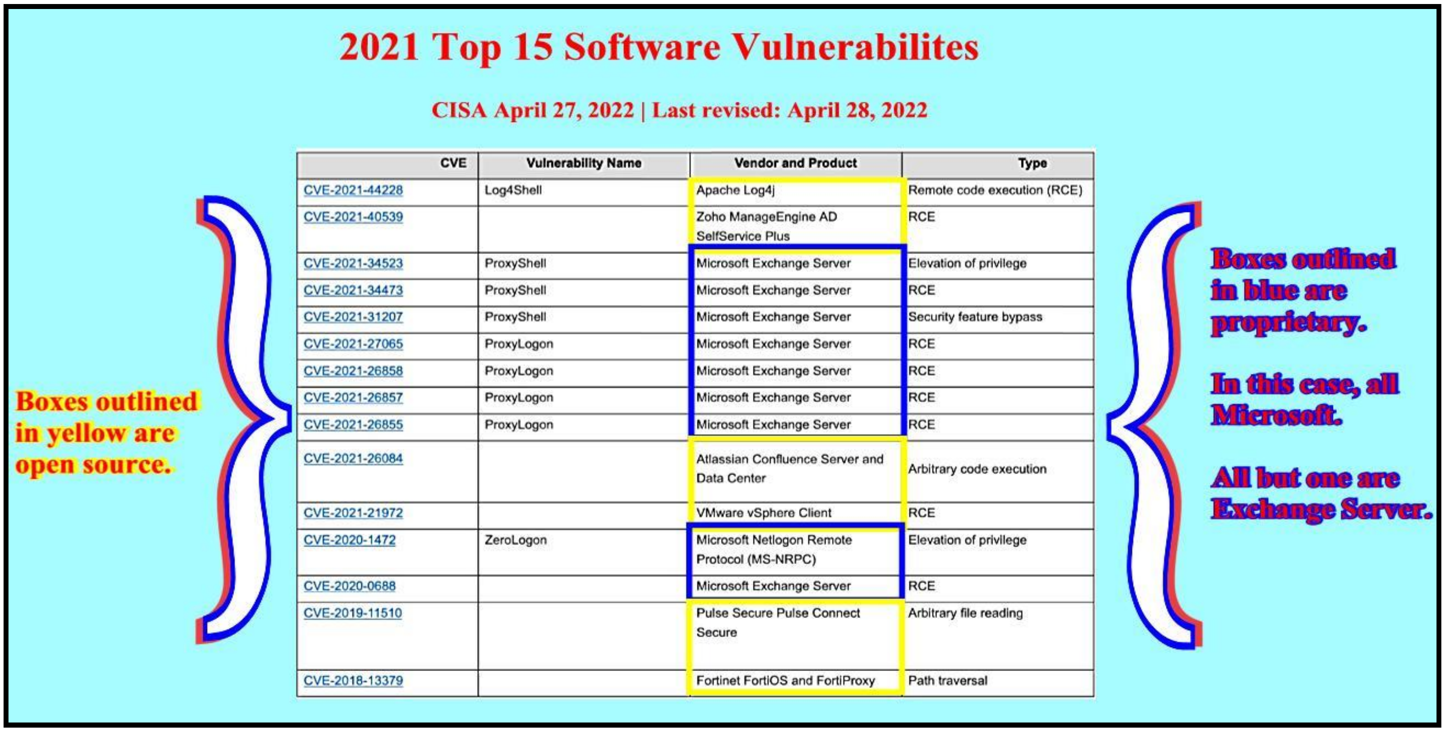
What brought open source software to the forefront of public discussions of the Internet was the Log4j debacle. The Log4j vulnerability was easy to exploit. A malformed string of characters could break the application. One of the first known exploits of Log4j were script kiddies. "**Some of the earliest attacks were kids pasting the malicious code in Minecraft servers**." But those kid games shortly became nation states exploiting the code. It is projected that despite all the patching, Log4j will remain a threat for as long as anyone can see. The logging software and its use are ubiquitous; but not all organizations will patch. Smaller organizations will simply not accept the downtime patching requires. The long term concern here is that criminals will remain active, but undetected in unpatched systems, and then use those hacked systems as platforms for future attacks. **Reporting by CNET, January 10, 2022**, expressed the long term threat Log4j represents thusly:

> **If left unpatched or otherwise unfixed, the major security flaw discovered a month ago in the Java-logging library Apache Log4j poses risks for huge swaths of the internet. The vulnerability in the widely used software could be exploited by cyberattackers to take over computer servers, potentially putting everything from consumer electronics to government and corporate systems at risk of a cyberattack.**

It is one thing for the federal government to dictate to its own department heads, "Patch or else!" The US government cannot, however, compel US private industries to temporarily shut down their operations and install these recommended patches to their systems. Moreover, the complexity of effective patching software has become an hindrance to patching for small and medium sized businesses. The admins in smaller enterprises may not know how to install the patches. Moreover, with **an increasing number of information workers of all types now working remotely, effective patching is even more problematical.**

> **“Work from home and remote work have brought a real and significant shift in the way medium- and large-size companies have to think about and perform patching... Almost all of our endpoints and workstations now are outside of the protections corporate networks offered. This makes it harder to reach and verify that computers have been patched.”**

Of course, it is not just vulnerabilities in open source Java based applications that are now considered threats if not patched. A release dated April 27, 2022, updated 4/28/2022, listed the **2021 Top Routinely Exploited Vulnerabilities**. **Of the top 15, applications listed, 6 are open source, and 8 are Microsoft products**. Of those 8 Microsoft applications, 7 are the same application, the Exchange Email Server.



2021 Top 15 Software Vulnerabilites

CISA April 27, 2022 | Last revised: April 28, 2022

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-44228	Log4Shell	Apache Log4j	Remote code execution (RCE)
CVE-2021-40539		Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523	ProxyShell	Microsoft Exchange Server	Elevation of privilege
CVE-2021-34473	ProxyShell	Microsoft Exchange Server	RCE
CVE-2021-31207	ProxyShell	Microsoft Exchange Server	Security feature bypass
CVE-2021-27065	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26858	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26857	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26084		Atlassian Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972		VMware vSphere Client	RCE
CVE-2020-1472	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688		Microsoft Exchange Server	RCE
CVE-2019-11510		Pulse Secure Pulse Connect Secure	Arbitrary file reading
CVE-2018-13379		Fortinet FortiOS and FortiProxy	Path traversal

Boxes outlined in yellow are open source.

Boxes outlined in blue are proprietary.

In this case, all Microsoft.

All but one are Exchange Server.

This chart above points out the primary difference between open source and proprietary software. There many different sources of open source software. Who is going to patch and how quickly becomes the crux of the problem. Ransomware has been documented to encrypt an infected system's files within 5 minutes. Both open source software and proprietary often share similar vulnerabilities. "**Both involve poorly written code, leaving "holes" or gaps that attackers can use to carry out malicious activities, such as modifying the code to extract sensitive data or damage the system**," as reported by Security Today, Aug 19, 2019.

When Microsoft becomes aware of a problem within one of their products, as the article referenced above states, "**a dedicated staff of professional developers is behind proprietary software, writing the code according to the directives of their organization**." So we can rely on the fact that Microsoft and its legion of coders will fix the problems as they arise. As was the case with the PrintNightmare, Microsoft will continue to work to get its patches right. Also, as the article states: "**On the other hand, open-source is, well, "open," meaning anybody can write, fix and maintain the projects**." Yet, it has been estimated that 96% of enterprise applications are run with some variation of open source software. Although that statistic is from a study done in 2018, it is still widely cited today.

So the open source software and applications that powers the Internet, and thus commerce and governments the world over, is not going to be replaced any time soon, nor could such a replacement be made without even more supply chain disruptions. Nevertheless, the situation as it stands has caused, and will continue to cause, supply chain disruptions, that most western leaning governments agree will only be exasperated by the war in Ukraine and whatever else may have lurking in his deluded mind.

Log4j was the catalyst for a reevaluation of how open source software threatens industries far afield from data management. December 16, 2021, writing for security vendor, Endpoint, George V. Hulme, detailed how attacks on supply chains impact everyone within that distribution chain. "**As organizations use open source to create applications, or use it within commercially available software, which contains as much as 90% open-source code itself, they're introducing a scary amount of third-party risk into their environment.**"

> **Here's how supply chain hacks work. Rather than targeting organizations directly, cybercriminals and nation-state hackers target software makers and software services providers. They inject attack code into software that is then used by other organizations. These attackers specifically target vulnerable software development pipelines and insecure cloud configurations, or they exploit software update processes.**

It is my contention that soon, maybe within months as the war drags, as criminal and hacktivist groups on every side seek to exploit what are ubiquitous and highly vulnerable systems, that these vulnerable systems will have to be taken off line and effectively patched. Any number of actors could force this action. And there will be a cost for such necessary and rapid mitigation and remediation efforts. As Hulme also wrote:

> **Managing open-source software risks requires security teams to closely examine the software's code. That doesn't mean just checking for known vulnerabilities and believing there's an all-clear if all patches are up-to-date... Instead, security teams must look at all of the components and the software dependencies within an open-source project, and understand how the various components have been assessed and tested for security vulnerabilities.**

What is being proposed here are more stringent quality controls be applied to open source software, and similar to those quality controls of proprietary software vendors. Deeper examinations of the source code could reveal defects that cannot be remedied. Adobe discontinued Flash. Microsoft is fervently trying to discontinue Internet Explorer. Those popular applications could simply not be fixed. If that happens to a critical piece of open source — it is deemed to be broken beyond all repair — the effects of such a supply system breakdown could well be devastating.

This is not simply a topic relegated to the tinfoil hat and propeller head class. No less a prestigious business publication as, ***The Harvard Business Review***, published an article May 2021, that asked the question: **Is Third-Party Software Leaving You Vulnerable to Cyberattacks?** And the HBR article makes my case:

> **When companies buy digital products, they expect them to be secure. In most cases, they don't test for vulnerabilities down the digital supply chain — and don't even have adequate processes or tools to do so. Hackers have taken note, and incidents of supply chain cyber-attacks, which exploit weaknesses within the digital supply chain to break into organizations' internal networks, are on the rise. As a result, there have been many headline incidents that not only bring shame to the companies involved, but rachet up the visibility of these threats to top executives who want to know their offerings are secure.**
>
> **Leaders need new ways to reduce supply chain cybersecurity risks, whether they're buying digital products and or producing them.**

The problem has been identified by all those with a stake in modern day distribution of goods and services. Implementing solutions that will stick will require actions that can cause as much temporary disruptions as the attacks themselves. We are, however, as a society, a nation, and a community of users, way past singing the same ol blues about the same ol problems. Solutions will be implemented. And somewhere up and/or down the distribution line, real people will suffer the fallout from finally fixing real problems long know about, but left to fester. And why were these problems left to fester? When everyone and anyone is responsible for mitigation and remediation, then really no one is responsible for mitigation and remediation.

The sound you hear is the paradigm shifting as the Titans of American Industry, circa 2022, having a come to Jesus moment about the infrastructure their business empires are so uneasily perched upon. See cartoon above.

Back to Top

Gerald Reiff

Back to Top

next post →