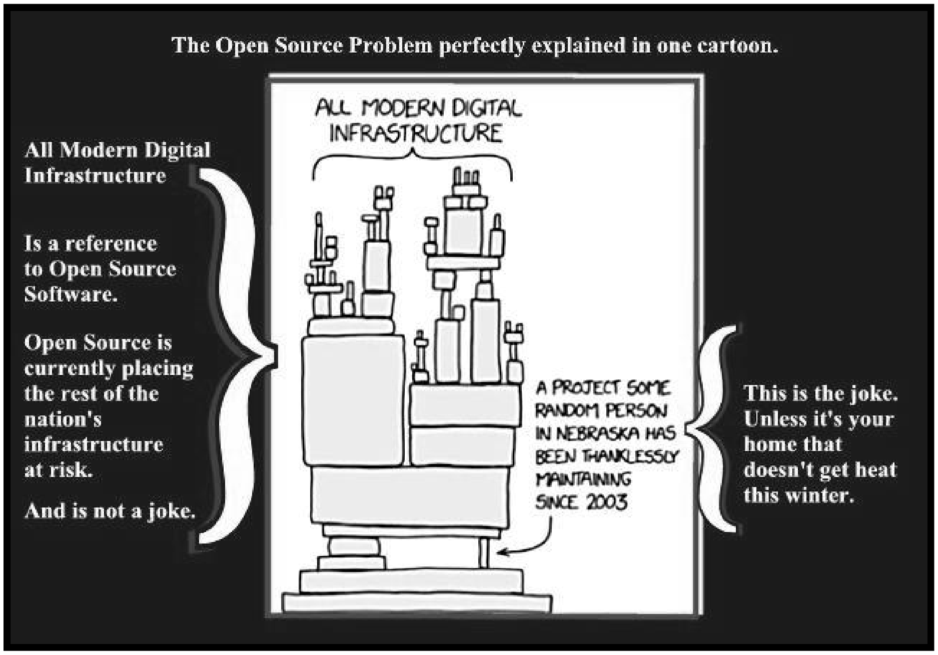
Top

Newsletter 6/22/2022

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, Part Deux

Now as I was saying before I was so rudely interrupted...


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.

That the open source software that powers much of today's industrial infrastructure must be reevaluated from a security viewpoint is now apparent to decision makers across many different sectors of the world economy. It has been reported that **"software supply chain attacks grew by more than 300 percent in 2021 in comparison to 2020." A supply chain attack is best defined as**:

> **A supply chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain.**
>
> **Software supply chain attacks inject malicious code into an application in order to infect all users of an app, while hardware supply chain attacks compromise physical components for the same purpose.**

The CrowdStrike article cited above makes the salient point that "**Software supply chains are particularly vulnerable because modern software is not written from scratch: rather, it involves many off-the-shelf components, such as third-party APIs, open source code and proprietary code from software vendors."**

The very real example of a software supply chain attack would be when a managed service provider (MSP) is the subject of a cyberattack. So alarmed are certain major Western economies about the impact of cyberattacks against Software as a Service (SaaS) and cloud service providers, to name only a couple of such providers, that on May 11, 2022, the NSA, CISA, and the FBI, along with their equivalent agencies from United Kingdom (NCSC-UK), Australia (ACSC), Canada (CCCS), New Zealand (NCSC-NZ), issued a joint statement that stated the agencies cited "**are aware of recent reports that observe an increase in malicious cyber activity targeting managed service providers (MSPs) and expect this trend to continue.** " In the CISA press release cited above, how and why the security of MSPs is now considered so critical is detailed.

> **MSPs provide services that usually require both trusted network connectivity and privileged access to and from customer systems. Many**

> **organizations—ranging from large critical infrastructure organizations to small- and mid-sized businesses—use MSPs to manage ICT systems, store data, or support sensitive processes. Many organizations make use of MSPs to scale and support network environments and processes without expanding their internal staff or having to develop the capabilities internally.**

Or put more succinctly in a Press Release issued the same day by the NSA: "**MSPs make attractive targets for malicious actors, including nation-state actors, because compromising an MSP network allows for access to and compromise of the provider-customer trust relationships**."

Of course, developers of open source software based projects are themselves increasingly aware of the security risks of their products. In one survey of software developers, **"54% of survey respondents said their firm knowingly releases software with potential security risks."** In the same survey, **"98% of respondents said that using third-party software, including open-source software increases security risks."**

A very current and real world example of how a device built upon vulnerable open source is the example of **Siemens SINEC network management system (NMS)**. Siemens NMS is an example of "**Open Platform Communications (OPC) network protocol." The purpose of which is explained below**:

> **Siemens' SINEC NMS is a popular tool used by operators to understand how Siemens control systems and operations are functioning on the network, how they're connected and dependent on one another, as well as their status. The diagnostics and network topology generated by the tool allow operators to see and respond to events, improve configurations, monitor device health, and carry out firmware upgrades and configuration changes.**

The article referenced above shows a screen shot of the Siemens' SINEC NMS. The image displays a Windows Network type layout. The display is an example of the "**diagnostics and network topology generated by the tool allow operators to see and respond to events, improve configurations, monitor device health, and carry out firmware upgrades and configuration changes.**" Thus, access to Siemens' SINEC NMS control panel would also provide access to the entire network.

Researchers have found 15 separate vulnerabilities in the Siemens' SINEC NMS.

> **Team82 researched Siemens SINEC and found 15 unique vulnerabilities, that could allow a user to escalate their permissions, gain administrative rights to the system, leak sensitive information, cause a denial of service on the platform, and even achieve remote code execution on the hosting machine using NT AUTHORITY\SYSTEM privileges.**

The programming language behind the Siemens' SINEC NMS is **JavaSpring**. We might remember that vulnerabilities in a Java Library launched the Log4J debacle.

Another current example of third party software embedded into controls of critical infrastructure are vulnerabilities in the embedded software that controls automated access to many otherwise secure installations. June 9, 2022, researchers had published a report that detailed "**four zero-day security vulnerabilities have been disclosed in the HID Mercury access controller system that's used widely in healthcare, education, transportation, and government facilities**."

"More than 20 OEM partners provide access control solutions with Mercury boards. " So any one of the reported vulnerabilities in the HID Mercury access controller could result in the physical unauthorized access to denial of legitimate access to critical installations. As has been noted by security vendor **Trillex,** "**by chaining two of the aforementioned weaknesses, it was able to gain root-level privileges on the device remotely and unlock and control the doors, effectively subverting the system monitoring protections**."

Certainly unauthorized control of the physical locking mechanism to keep the right technicians out and remotely let the wrong techs in would absolutely be disruptive to whatever legitimate activity might occur at the compromised installation.

Again, the appropriate mitigating response is for the admins of these systems to patch their vulnerable systems. And responsible operators will make every effort to do so; irresponsible operators won't patch. Many simply won't have the technical capacity patch. Any unpatched networked device is a threat to the entire network. If that unpatched device controls the water treatment plant in a smaller municipality without the big city resources then the entire town could be at risk from the fallout of a cyber attack.

This is our world today. It is not possible to simply replace the existing software used in these critical industrial controls. This is why it is imperative that any vulnerability in any widely used software be patched immediately upon notice of the vulnerability and its mitigation. And this information should be widely disseminated. The failure to do so can literally put the lives of many at risk.

These systems impact everyone at one time or another.

Back to Top

Gerald Reiff

Back to Top

next post →