Fortress

REPORT

A Software Supply Chain Dependent on Adversaries

Research shows 90% of US Infrastructure contains code from adversaries

Introduction

The United States is under attack. Hostile nation-states have America's critical infrastructure in their crosshairs. Highly desirable potential targets include America's power grid and the military. And instead of coming by air, land, and sea, this new generation of fighters now has the potential to get into America via our own technology – including components used to build software coming from American companies. These components make up the software used in power grid substations, military facilities, and even by consumers in their homes.

New research from Fortress Information Security found that 90% of software products used to manage the U.S. power grid contained code "contributions" from Russian or Chinese developers. These contributions are commonly found on software development platforms. Additionally, the study found software with contributions from Russian or Chinese developers is 2.25 times more likely to have vulnerabilities and three more times likely to have critical vulnerabilities.

Just one compromised component can have devastating effects. The Log4Shell vulnerability continues to cause problems for security teams more than a year and a half after its discovery. The U.S. Cybersecurity & Infrastructure Security Agency (CISA) said in 2021 "Log4Shell is especially critical because it allows malicious actors to remotely run code on vulnerable networks and take full control of systems." Late in 2022, Tenable determined nearly three-quarters of all organizations remained at risk one year after Log4Shell's discovery. Around the same time, Arctic Wolf Labs found Log4j exploitations made up 11% of its incident response cases, with the average cost for incident response amounting to $90,000.

Our researchers estimate that it could cost as much as $40 billion to replace the questionable and bad code now out in the wild. *

The Log4Shell crisis provided new urgency for government and Industry leaders to push for the adoption of Software Bills of Materials (SBOM), commonly known as SBOMs. An SBOM is like an ingredients list, telling users what components make up the software's code, and providing transparency into what's inside the software in use. SBOMs could have also helped security teams track and mitigate damage resulting from the 2020 SolarWinds attack and, more recently, attacks in which threat actors exploited vulnerabilities in MOVEit software applications.

Log4J and SolarWinds spurred CISA to provide more transparency for all organizations, particularly for government agencies and critical infrastructure companies. The research in this paper wouldn't be possible without CISA's commitment to ensuring the broad implementation of SBOMs. Other leading cybersecurity entities have also made clear their support for SBOMs. The widely cited Log4j review by the Cyber Safety Review Board pointed to SBOMs as a critical tool to prevent future cyber calamities and that "addressing SBOM standardization gaps would support a faster software supply chain vulnerability response." The bipartisan Cyberspace Solarium Commission urged the federal government to require SBOMs for software it purchases.

Despite all the support from respected cybersecurity minds, organizations are struggling to implement SBOMs. Recent research from the cloud-native application security provider Snyk surveyed 404 technical employees at organizations ranging from

*Source: Fortress SBOM Use Cases for Asset Owners Whitepaper, August 2023, https://www.fortressinfosec.com/en-us/sbom-use-cases-for-asset-owners

Introduction

small companies to large multinationals. Snyk found just 42 percent of organizations are using SBOMs. That's an improvement. The technological research and consulting firm Gartner found in 2022 that only 5 percent of organizations had adopted SBOMs. For these reasons, Fortress felt it was important to share its research pulled from looking at publicly available SBOMs. Fortress's findings are alarming and demonstrate the need for broad SBOM adoption quickly to mitigate and prevent attacks on critical infrastructure organizations.

Methodology

Starting in 2022, Fortress looked at roughly 900 kinds of software most used by electric power companies, including information technology (IT) products, used for network management, and operational technology (OT) products, used for business functions. This included products from large well-known vendors like feeder terminals, chromatographs, network switches, management relays, and routers. The researchers pulled 392 files that used multiple complementary tools for firmware and binary analysis. From those files, they were then able to create 224 SBOMs. They looked at mostly open-source code. Gartner has estimated that "40% to 80% of the lines of code in new software projects come from third parties (for example, runtime, libraries, components and software development kits [SDKs])."

71 percent of the analyzed product software was the most up-to-date version available. However, some older versions were included to make a more realistic population set of products a utility might have in their environment. Two tools were used to analyze the files and produce a Software Bills of Materials (SBOM) for the product. One tool specialized in firmware, the other in other types of binary files. Once SBOMs were created statistics were produced on the average number of vulnerabilies per product, CVSS severity score, and time since the disclosure. Additionally, data was collected on the location of contributors to these components by reviewing open-source component repository information.

Developers from U.S. Adversaries Make Significant Contributions to Software Products

Almost all the software products commonly used by U.S. utilities contain code contributions from Russian and Chinese developers. Researchers also found contributions from Cuba, Iran, and North Korea.

When Fortress researchers looked at all 7,918 components they reviewed, 13% had contributions from Russian and Chinese developers. 90 percent of the products used to manage America's energy grid contained component contributions from developers saying they were from Russia and China.

Additionally, software with Russian or Chinese-made code examined by Fortress research is 2.25 times more likely to have vulnerabilities. Perhaps even more troubling, that software is three times more likely to have critical vulnerabilities – the vulnerabilities that are easiest to exploit and more likely to allow damage to hardware.

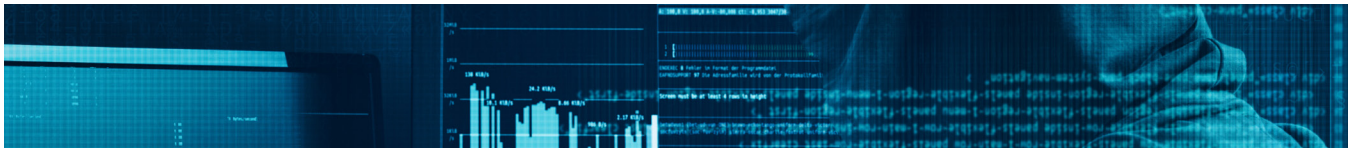
To be clear -
researchers only counted components with contributions as coming from Russia, China, or any country if the creators acknowledged their country of origin. Only those developers who self-identified on a software development platform as being from a country were put on that country's list. There is no information on the platforms indicating that the code resulted from a state-sanctioned project. Fortress experts see a clear correlation between the increased vulnerabilities in some contributions and the country of origin but cannot yet establish if the country of origin is the cause of the higher number.

Several well-known components contain contributions coming from Russian and/or Chinese developers, including:

- **Open SSL**
  A software library for applications for general-purpose cryptography and secure communication. Researchers found the OpenSSL component in 58% of the OT/IT products they reviewed. It contains 10 contributions from China and three from Russia.
- **Busy Box**
  A software suite that provides several Unix utilities in a single executable file.It was specifically created for embedded operating systems with very limited resources. Researchers found this component in 44% of the OT/IT products reviewed. It contains three contributions from China and four from Russia.
- **U-Boot**
  An open-source primary boot loader used in embedded devices to package the instructions to boot the device's operating system kernel. Researchers found U-boot was found in 9% of the OT/IT products reviewed. U-boot has eight contributions from China and two from Russia.

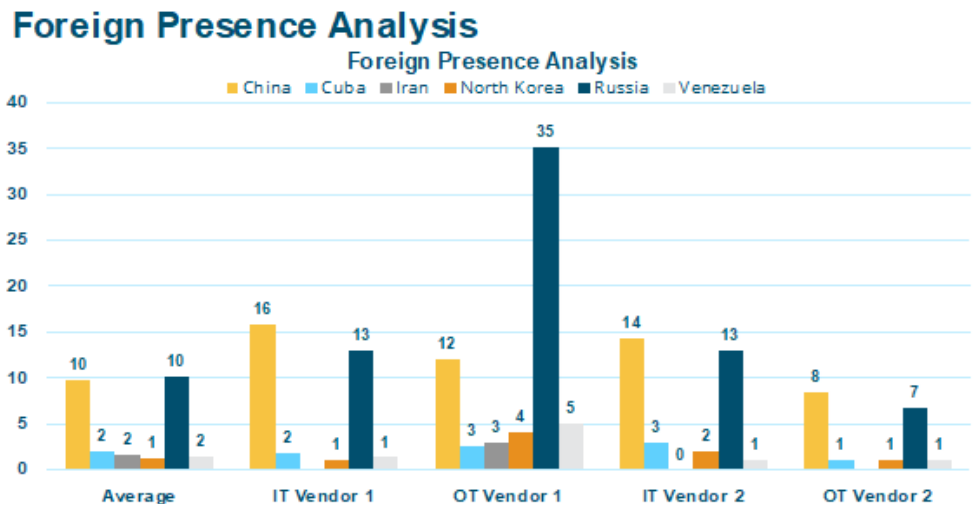
There's additional insight on critical vulnerabilities in components later in this report.

There's no reason to believe that any of the three component makers here - as well as many other researchers found with suspect code - are working to undermine the United States and/or helping a nation-state that is hostile to the US. The components mentioned above, and others studied by Fortress researchers could be the first victims in a chain of targets potentially compromised as a result of the foreign-made code.



Developers from U.S. Adversaries Make Significant Contributions to Software Products

Almost all the software products commonly used by U.S. utilities contain code contributions from Russian and Chinese developers. Researchers also found contributions from Cuba, Iran, and North Korea.



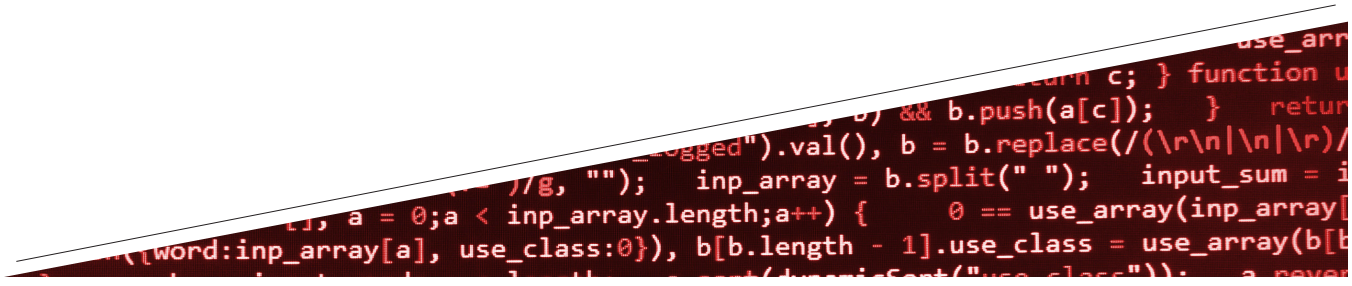
The slide above shows the average number of components containing code contributions from high-risk countries, such as China, Cuba, Iran, North Korea, and Russia, compared to a selection of popular IT and OT vendors.

Researchers found an average of 10 contributions from Russia and China per vendor. The series on the left is the average number of components of concern. Researchers picked four vendors – 2 IT and 2 OT - to compare to the average. These are large, well-known IT and OT vendors.

The graphic shows that there is variance between vendors – with some having large amounts of components with influences from high-risk countries, while others had just a few.

Leaders in Washington have made it abundantly clear just how dangerous China can be. The Office of the Director of National Intelligence's (DNI) 2023 Annual Threat Assessment said: "China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks.

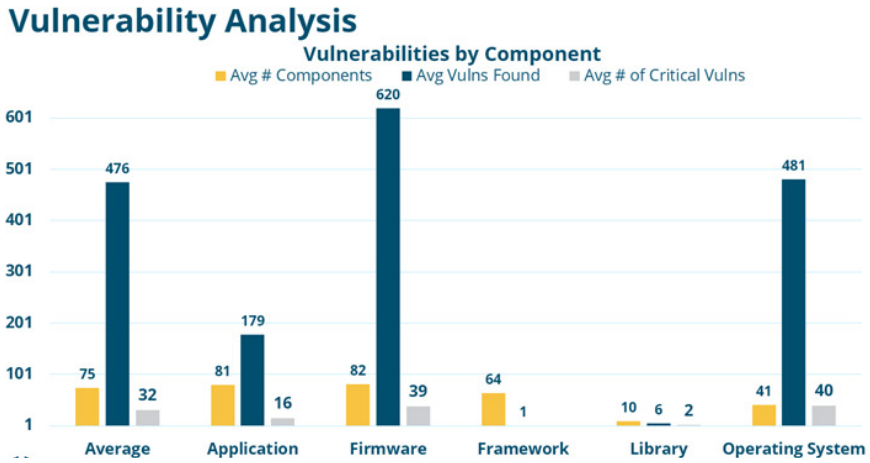
China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland. . . China almost certainly is capable of launching cyberattacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems." The DNI's report said Russia "is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis."



Significant Vulnerabilities Found – Some Benign, Others Critical

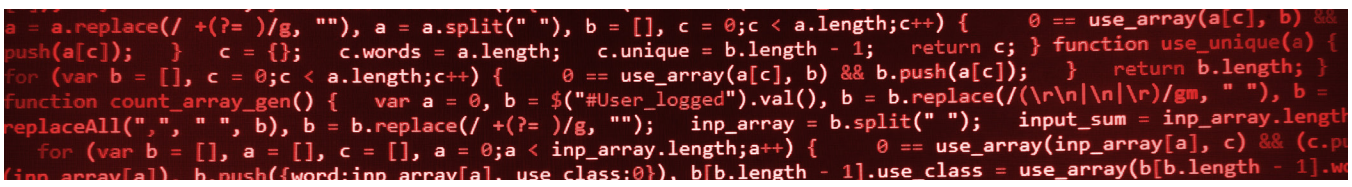
Firmware had the most vulnerabilities with an average of 620 vulnerabilities per product, but operating systems had just as many critical vulnerabilities – with 12% being critical. Firmware can be its own mini operating system to run these devices, Typically the firmware we found is Linux-based and was not running the most up-to-date versions of the linux_kernel or the other included components.

In all, approximately 7% of all vulnerabilities were critical – the vulnerabilities that should be prioritized for remediation. 12% of operating system vulnerabilities were critical.



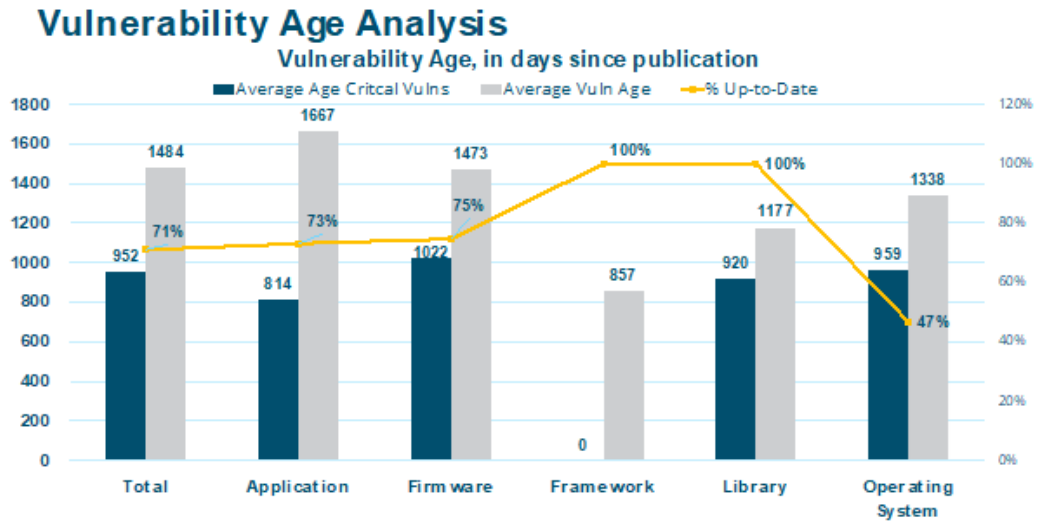
The vulnerabilities can live in different parts of the software. The graphic above looks at where researchers found them.

The yellow bar is the average number of components found in an SBOM for that file type. The blue is the average number of vulnerabilities found. This includes all severity types, Critical, High, Medium, and Low. And the gray bar is the average number of critical vulnerabilities found in each product.



Vulnerabilities in Software Can Lie in Waiting for Years for Detection

Perhaps even more concerning, SBOM analysis showed that vulnerabilities built into the software running important operations and components lie in wait for longer than four years – without getting attention from vendors, suppliers, or utility providers.



SBOM analyses by Fortress researchers showed that vulnerabilities built into the software running critical operations and components lie in wait for longer than four years – without getting attention from vendors, suppliers, or utility providers.

The gray bars represent the average age of all vulnerabilities, generally several years old. The blue bars note the average maximum age for each product.

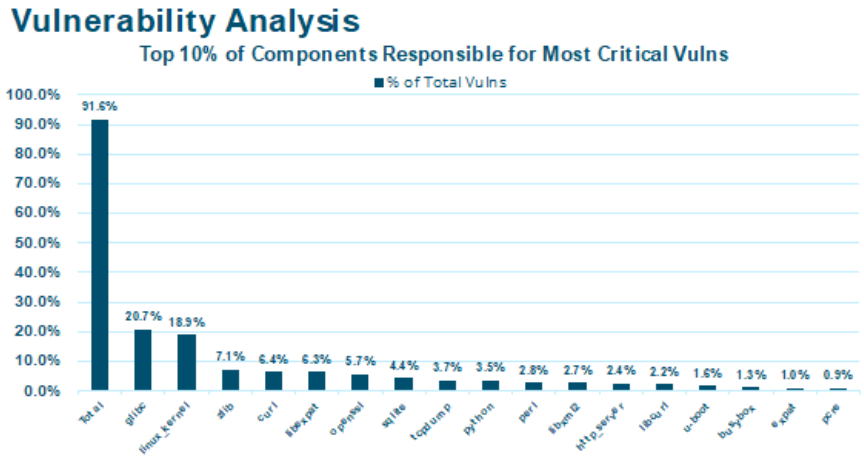
The yellow line shows what percentage of products studied were the most up-to-date versions of the software available.

The average age of critical vulnerabilities was nearly three years – 952 days.

Organizations would benefit from VEX (Vulnerability Exploitability eXchange) information, which would show if an organization were affected by this older vulnerability or if there is a configuration that mitigates the issue. VEXs are companion documents to SBOMs to fill vulnerability management needs. While SBOMs help you illuminate what vulnerabilities could be affecting your products, VEX documents explain whether a product is affected by a vulnerability identified in a component.

Fixing a Few Vulnerabilities Will Make a Big Difference

Ten percent of components are responsible for 92% of the most critical vulnerabilities. Two components, glibc and linux_kernal, were responsible for around 40% of these potential vulnerabilities.



Focusing on a small number of components for updates and patches will resolve 92% of critical vulnerabilities.

The chart above shows the 10% of components responsible for the most critical vulnerabilities. Two components, glibc and linux_kernal, combined were responsible for around 40% of these potential vulnerabilities.

Patching 17 components resolved 92% of the critical vulnerabilities found, showing a large risk reduction from updating a small number of components.

5 Ways to Secure the National Power Grid

The age of the developer who writes long strings of code is over. Increasingly, we rely on open-source communities where components like Log4J are built from contributions shared between developers who have never met. Sharing contributions to build components does produce software that works effectively and is relatively easy to use. However, curating contributions from various sources of unknown origin – then passing along those contributions even though they may have only the most cursory review for security flaws – dramatically increases the likelihood of building vulnerable, insecure software.

The team at Fortress Information Security makes the following recommendations:

Universal Adoption of SBOM

As mentioned previously, research by Snyk and Gartner showed that SBOM adoption has been too low. However, there are encouraging signs from both surveys. Snyk did find that 31 percent of respondents said their organizations plan to adopt SBOMs soon. And that troubling number from Gartner is expected to change dramatically – the company estimates "by 2025, 60% of organizations building or procuring critical infrastructure software will mandate and standardize SBOMs in their software engineering practice." But those numbers are still way behind where they need to be. It just takes a backdoor, in one company, in one critical sector, to give bad actors an opening into the systems running critical services, like the power grid.

SBOMs will help make it easier for security analysts to identify bad code. An SBOM would include proprietary code as well as open-source and third-party components. There is widespread agreement among government leaders, company executives, academics, and security experts that SBOMs are desperately needed as threat actors continue aggressive, troubling attacks. Until we have secure-by-design software, we'll need SBOMs just to hold our own with attacks.

Additionally, CISA is working on producing a Secure Software Self-Attestation Common Form for government vendors. This document will require software producers supplying products to the federal government to guarantee the implementation of specific security practices. Software makers will either have to promise the products are being tested or have a specific timeline for testing to occur. An executive with the software maker will sign the document. If a company doesn't have an SBOM and/or the Attestation Common Form, the government agency would be required to look at other products that demonstrate that commitment to security. When this document is complete, critical infrastructure companies should consider requiring the same document, before the government mandates a similar action. The best solutions come from those of us in the security space. Once a reasonable and robust standard is developed, then all parties can work with the government to devise sensible enforcement mechanisms. If the industry takes steps to require SBOMs and Attestation forms voluntarily, the less the government will have to mandate them.

Cybersecurity as a Key Procurement Criteria

There are signs from Washington demonstrating the federal government's commitment to SBOMs. The White House's Executive Order 14028 mandates government agencies have SBOMs for software they purchase beginning in 2024. CISA has at least five working groups meeting weekly dedicated to developing best practices and standards in key industries. This is necessary. Federal Times recently reported that more than two-thirds of cabinet-level agencies maintain public code repositories.

Also worth noting, CISA is working with Japan and European countries on common standards to make compliance easier. This work will help ensure software makers are not creating multiple versions of one product to satisfy different procurement standards in other countries.

Clear Guidance from the Federal Government and Regulators on Best Practices

While the adoption numbers are low, we at Fortress consistently hear from organizations that want to implement an SBOM program. However, those same organizations want more certainty from the federal government on what a program will require. Congress's decision in 2022 to remove language from the National Defense Authorization Act (NDAA) that would have required software makers to include an SBOM on products offered to federal agencies certainly muddied the picture.

The government has identified 16 critical infrastructure industries that must make sure they can purchase software with SBOMs. CISA says the 16 industries have "assets, systems, and networks, whether physical or virtual, and are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."

Below is a table of those 16 industries:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food & Agriculture
- Government Facilities
- Healthcare & Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water & Wastewater Systems

However, the timetable for companies to have SBOM programs in place isn't entirely clear.

Federal Times reported The National Cybersecurity Strategy Implementation Plan (NCSIP) includes a target in 2025 to "develop a process for closing gaps in SBOMs and shoring up unsupported software in critical infrastructure." But the same story points out that the lack of specifics makes it difficult for the private sector to act.

Washington must provide clarity on implementation. The aforementioned private-sector numbers might be considerably better if buyers knew what products would satisfy federal requirements.

Federal Government Regulation of Software Development Platforms

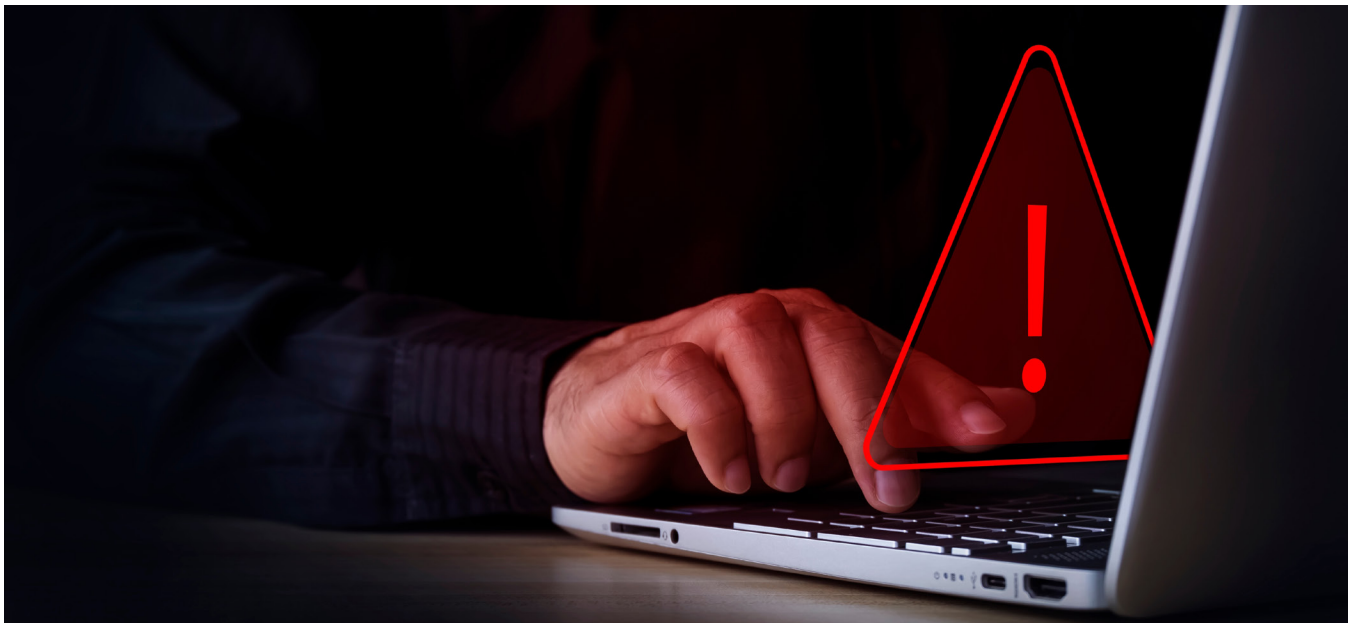
Additionally, America needs regulation of software development platforms – either from industry or from Washington. Right now, no one is monitoring where or what is in these open-source exchanges of code. Log4Shell made it clear – you can sneak code past companies. While organizations have taken extreme measures to fix problems resulting from Log4Shell, little has been done to prevent another Log4Shell from coming from one of the software development platforms.

On August 10, CISA put out a request to the open-source community asking for ideas on how to secure code from their community. The hope is to craft a report from these suggestions that could come out later this year. Companies and individuals must share as many good ideas as possible to get this done. CISA's leadership on securing software has been outstanding and the Agency's efforts to encourage both private-sector collaboration and industry solutions to solve this crisis are the right ways to attack this problem.

The software development community would do us all a great service if they joined the effort to ensure code contributions on the platforms are secure. Especially when those companies are trying to avoid a $40 billion-dollar tab. Nobody wants to create a situation where we need a software industry bailout, but we need the software industry to find solutions instead of fighting SBOM legislation – which reportedly their lobbyists did before the SBOM provision was pulled from the NDAA.

Software Developers Adopting Secure by Design

Until we have confidence that software isn't laced with malicious code, every software product could contain a ticking time bomb. SBOMs provide us with the best tool to find compromised components, but the best solution will ultimately be designing products that are secure from the outset. That won't happen if software makers pull contributions from parts unknown. There must be a better way.



Securing critical supply chains and cyber assets from evolving threats.
Fortress. Absolutely Critical.

Find out more at **fortressinfosec.com**