EINPRESSWIRE

Enabling Zero Trust in the Software Supply Chain

To combat supply chain threats, a combination of technical and behavioral techniques can help thwart our adversaries and protect our nation's data networks.

HERNDON, VIRGINIA, UNITED STATES, April 18, 2024 /EINPresswire.com/ -- By Kara Zajac, CISSP and William Smith, CISSP – Crimson Phoenix, LLC

Crimson Phoenix LLC, headquartered in the DC/Virginia area, provides supply chain management, recommendations, and improvements in support of multiple government programs and is pleased to contribute this article as part of April’s Supply Chain Integrity Month.

Providing cutting-edge data-enabled solutions to the Intelligence and Defense Communities.

Recent supply chain compromises have caused major organizations to rethink software security. A recent example was Log4Shell, a critical vulnerability within the Apache Log4j software package that allowed attackers to conduct Remote Code Execution (RCE) attacks on vulnerable software applications using this library. The Log4Shell vulnerability, CVE-2021-44228, affected over 38,000 unique applications and forced vendors to quickly create, test, and distribute patches to their software applications. Another major software supply chain compromise happened in 2020, when Russia’s Foreign Intelligence Service (SVR), compromised SolarWinds. This compromise resulted in a malicious software update to the Orion IT monitoring and management software distributed to 18,000 customers, including Cisco, VMware, Microsoft, and several government agencies. These supply chain threats highlight two critical issues that are difficult to fix. While this problem may seem expansive, a combination of technical and behavioral techniques can combine to thwart our adversaries and protect our nation's data networks.

The first example highlights issues with establishing and maintaining trust within the supply chain. The Log4Shell vulnerability was present in thousands of software applications already vetted and considered trusted. Difficulties in triaging and patching the vulnerability were exacerbated by the lack of Software Bill of Materials (SBOM) listing all application components. To remediate the Log4Shell vulnerability, thousands of software vendors had to update their applications and each organization had to download and apply those updates to their systems. This resulted in a race for organizations to identify all effected software applications in use and implement vendor patches when they became available. Many organizations took the approach of trying to apply patches as quickly as possible, issuing orders to mitigate the vulnerability within 30 days. This task is complicated by historically lengthy change management processes requiring multiple approvals before implementation on production systems.

The SolarWinds example illustrates another challenge with the current cybersecurity supply chain infrastructure. A malicious patch was introduced to production systems through signed and vendor-trusted software. The malicious patch was not identified within the lengthy patch and change management processes, demonstrating the default action is to trust the approved vendor.

Both incidents highlight the challenges with patch and change management best practices. These issues with supply chain security are compounded when vendors use open-source libraries within their software applications, particularly when a SBOM is not present. This makes it extremely difficult to secure the next link in the supply chain. In a Zero-Trust Supply Chain (ZTSC) environment, patches and applications are untrusted by default.

The US Government has provided multiple publications, frameworks, and architectures addressing threats within the software supply chain. Some of these publications include NIST SP 800-37r1 Risk Management Framework (RMF) and NIST SP 800-161r1 Cybersecurity Supply Chain Risk Management (C-SCRM). Both NIST documents detail strategies to protect the software supply chain, but neither document mentions zero trust as a solution. NIST SP 800-207 Zero Trust Architecture (ZTA) only mentions supply chains once.

Using these documents as a baseline, Crimson Phoenix can design a ZTSC model to mitigate further inadvertent threats, such as Log4Shell and the malicious SolarWinds update crafted by the SVR. Three strategies that enable ZTSC are patch management, micro-segmentation, and SBOMs.

Establishing comprehensive patch management strategies incorporating principles of zero trust, such as “never trust, always verify,” and applying those principles to the patch management process can reduce the chances of supply chain compromise from malicious software updates. The strategies for patch management should put comprehensive processes in place including scanning, evaluating, testing, and implementing patches into a sandbox environment before they are put into production. The patch management process should also empower system owners to be responsible for patching, but not seek approval for every change to their information system.

Micro-segmentation from ZTA can be implemented on systems and individual firewalls between systems on the network. Additionally, managing inbound and outbound rules with Allow Lists will ensure rogue communications are not possible. If an active internet connection is not needed, you should block the server from reaching the internet. For example, only 20-30 percent of all SolarWinds's Orion servers were online, reducing the number of infected servers that could reach back to SVR's command and control network.

An aspect of C-SCRM that should also be expanded is ensuring vendors providing software applications are providing an up-to-date SBOM for their product. The SBOM should include all software libraries and the versions of those libraries used within the application. By having an up-to-date and accurate enterprise-wide SBOM, organizations can proactively assess the risk that a vendor's application would create within the network. The difficulty here is commercial software vendors use open-source libraries to reduce cost and time when developing new software. This leads to the supply chain of trust going from untrusted open-source software libraries into a vendor and then into an organization as a trusted software vendor.

Application developers and maintainers must be aware of and take steps to mitigate product threats. The above processes will not mitigate all threats, but implementations of the ZTSC model will greatly reduce the potential damage of malicious and inadvertent threat actors in your organization.

About Crimson Phoenix
Crimson Phoenix provides cutting-edge data-enabled solutions to the Intelligence and Defense Communities, with a focus on artificial intelligence, machine learning, and digital technologies that enhance intelligence analysis to the forefront of innovation. More Information can be found at crimsonphoenix.com.

Silver Crawford, Vice President, Marketing
Crimson Phoenix, LLC
email us here
Visit us on social media:
Facebook
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/704318167