Visibility is vital if we are to improve safety and trust in open source, says Meterian

When it comes to securing open source, visibility and transparency are vital - and responding quickly to a vulnerability saves resource and reputations

Image by Kate Trysh, Unsplash

LONDON, UK, March 31, 2022 /EINPresswire.com/ -- Recent high profile cyber security incidents have reinforced the importance of cleaning up the open-source software supply chain. From Heartbleed to the Apache Software Foundation's Log4j vulnerability, these highly publicised incidents have exposed the threats associated open-source software.

They have galvanised a range of responses at national and international level - even prompted the White House to convene an Open Source Software Security Summit in January, attended by leaders from global technology companies including Google, Meta, Apple, and Cisco.

> Now is the time for organisations to implement integrated and automated tooling to gain comprehensive risk control of components in their open-source software supply chain."
>
> *Vivian Dufour, CEO, Meterian*

The gathering may have been precipitated by the Log4Shell vulnerability, but the wider context was clear. How do we ensure source code, build, and distribution integrity to achieve effective open-source security management?

Open source under the microscope

Technology companies have been using open source for years. It speeds up innovation and time to market but it also has unique security challenges. The responsibility of ongoing security maintenance is carried out by a community of dedicated volunteers. Yet these security incidents have demonstrated that the use of open source is so ubiquitous that no company can blindly continue in the mode of business as usual.

Apache Log4J software is an example. Used in software developments and security applications across the world, the zero-day vulnerability in the software sent shockwaves across organisations as security teams scrambled to patch the flaw. If left unfixed, it meant potential attackers could break into systems, causing untold damage, not least to brand reputations.

Improving safety and trust when speed is of the essence

However, how do you quickly patch what you don't know you have? If we are to increase safety and trust in software, we must improve transparency and visibility across the entire software supply chain.

Companies should have the ability to automatically identify open-source components in order to monitor and manage security risk from publicly disclosed vulnerabilities. A software bill of materials (SBOM) should be a minimum for any project or development. Without such visibility of all component parts, security teams cannot manage risk and will be unaware, and potentially exposed, to dangers lurking in their software.

Innovating securely
Organisations can and should take advantage of the many benefits that open-source software can deliver, but they must not do so blindly.

Now is the time for organisations to implement integrated and automated tooling to gain comprehensive risk control of components in their open-source software supply chain. Only by increasing visibility, coverage of known unknowns and transparency can companies stay one step ahead.

To find out more or to read the full article, click here:

Vivian Dufour is CEO of Meterian.

Andreina West
PR Artistry
+44 1491 845553
email us here