Google will start distributing a security-vetted collection of open-source software libraries



Google announced a new initiative Tuesday aimed at securing the open-source software supply chain by curating and distributing a security-vetted collection of open-source packages to Google Cloud customers.

The new service, branded Assured Open Source Software, was introduced in a blog post from the company. In the post, Andy Chang, group product manager for security and privacy at Google Cloud, pointed to some of the challenges of securing open-source software and stressed Google's commitment to open source.

"There has been an increasing awareness in the developer community, enterprises, and governments of software supply chain risks," Chang wrote, citing last year's major log4j vulnerability as an example. "Google continues to be one of

the largest maintainers, contributors, and users of open source and is deeply involved in helping make the open source software ecosystem more secure.”

Per Google’s announcement, the Assured Open Source Software service will extend the benefits of Google’s own extensive software auditing experience to Cloud customers. All open-source packages made available through the service are also used internally by Google, the company said, and are regularly scanned and analyzed for vulnerabilities.

“There has been an increasing awareness in the developer community, enterprises, and governments of software supply chain risks.”
Currently, a list of the 550 major open-source libraries being continuously reviewed by Google is available on GitHub. While these libraries can all be downloaded independently of Google, the Assured OSS program will see audited versions distributed through Google Cloud – mitigating against incidents where developers intentionally or unintentionally corrupt widely used open-source libraries. At present, this service is in early access mode and is expected to be made available for wider customer testing in Q3 2022.

The announcement from Google comes as part of an industry-wide drive to improve the security of the open-source software supply chain and one that has also been supported by the Biden administration.

In January, a group of some of the nation’s largest tech companies met with representatives of federal agencies including the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency to discuss open-source software security in the wake of the log4j bug. Since then, a recent meeting of the companies involved resulted in a pledge of more than $30 million in funding to boost open-source software security.

Besides contributing funding, Google is also putting

engineering hours toward keeping the supply chain secure. The company recently announced the formation of an “Open Source Maintenance Crew” that would work with the maintainers of popular libraries to improve security.

https://www.theverge.com/2022/5/17/23097529/google-assured-open-source-software-security-vetted-libraries