GUIDE

Your next step is to compile a list of known vulnerabilities that have been reported against the open source components you've inventoried.

Most DIYers will use the U.S. government vulnerability disclosure database, the National Vulnerability Database (NVD), as their primary source. But be aware that not all vulnerabilities are reported to the NVD. Also, the format of NVD records often makes it difficult to determine which versions of a given open source component are affected by a vulnerability.

Other useful sources of information include project distribution sites, such as those maintained by the Debian and Python projects. Security blogs and message boards, such as the US-CERT alerts page and Google's security blog, should also be part of your daily abili

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com