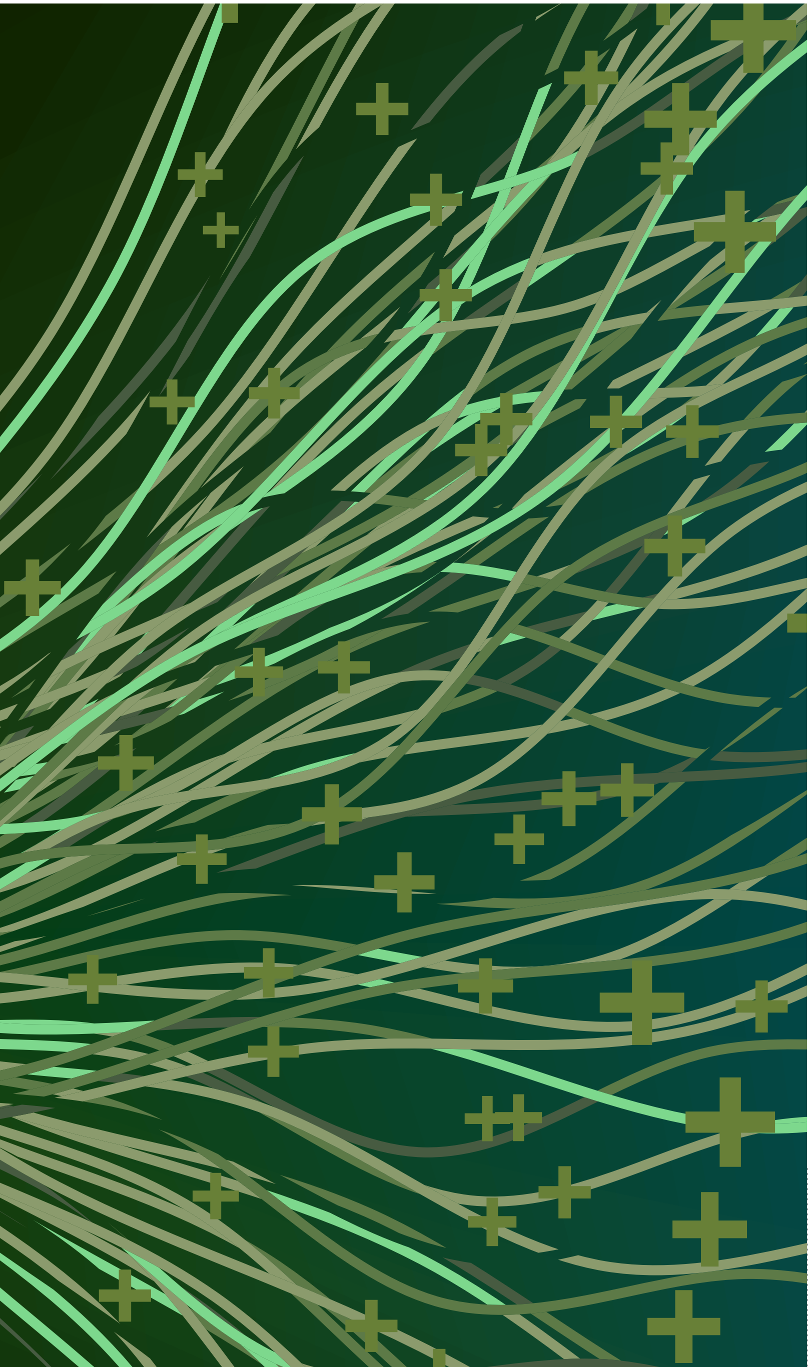
SearchSecurity



E-Guide

TAKE INVENTORY OF YOUR OPEN SOURCE SOFTWARE SECURITY

TechTarget

Home

Take inventory of your open source software security

DEVELOPERS LOVE REUSING code, whether it’s an open source library or a code snippet copied from the Internet. This expert tip looks at the best ways to secure and monitor component-driven software.

TAKE INVENTORY OF YOUR OPEN SOURCE SOFTWARE SECURITY

Michael Cobb

The majority of code in modern software applications is open source, pulled from the Internet for free and included in a project with just a couple of mouse clicks. To speed up build cycles, many developer tools and code compilers can automatically retrieve components and related libraries from the Internet and other repositories.

So what's the problem? Complex applications built this way pose numerous threats: A high percentage of open source components that are downloaded contain known security vulnerabilities, according to a 2014 Sonatype Open Source and Application Security Survey. Attackers can also compromise the host servers such as Sourceforge or GitHub and replace the open source components with malicious copies.

To mitigate the risks of vulnerable, and even malicious, components, enterprise development teams should create in-house repositories. This tip looks at the best ways for IT security to track and supervise the ongoing use of open source code to ensure it's a benefit, not a risk.

ONE CENTRAL LOCATION

An in-house repository provides a central point for the management of software components and their dependencies. Advanced repository systems allow IT security and development team managers to enforce policies regarding recycled code:

- Only approved components can be downloaded into the repository from a trusted source.
- Developers' tools must be configured to only allow usage of components from the in-house repository in assembled applications and other software projects.

This approach to open source software security removes the risk of compromised downloads from external repositories and ensures a validated and stable version of the code is available for use by enterprise developers.

Repository managers such as Sonatype Nexus and the open source Subversion can help integrate component lifecycle management into the application development lifecycle. These tools provide an inventory of the usage of open source components, many with complex dependencies, in internal repositories and production applications. In addition to alerting managers to any newly discovered vulnerabilities, repository managers make the ongoing monitoring of production applications easier – a major failing of many project teams.

USAGE POLICY AND GOVERNANCE

While a repository manager certainly simplifies component and code management, projects still need to be run with a policy in place to regulate code use and avoid any confusion over who is responsible for open source governance. Files that exist only in one central location greatly reduce a production application's or project's attack surface; however, IT security and development team managers should consider adding security wrappers around components to disable unused functionality. To ensure functions are used correctly, managers can restrict developer access to certain libraries, allowing only those who have passed relevant training modules or signed agreements to show they have read the appropriate documentation. Google, a major force in the open source

Home

Take inventory of your open source software security

movement, enforces a company-wide coding and comment style so developers can more easily follow each other's work, essential when thousands of developers are accessing a single monolithic code tree.

Many open source libraries and packages include example configurations and code snippets. While useful, they are often not written with security in mind as they tend to be simplified in order to explain how a function or feature works. IT security teams need to ensure developers don't simply cut and paste examples without having read the relevant documentation which, will cover security aspects of a function or settings in more depth.

Application developers should never assume that data has been correctly validated, especially if functions developed in-house receive data passed by a third-party component. The data may have been validated against a different set of requirements or rules. For example, a function to retrieve and display a user's telephone number from a database may accept + and () symbols, but if it then passes the data to another function that actually calls the number, these characters could cause the process to fail if they are not first removed.

EMERGENCY RESPONSE PLAN

The Open Web Application Security Project (OWASP) has flagged recycled code as a major vulnerability in the application development process. As application developers grow more dependent on open source components, the security problems will only get worse if steps aren't taken to control their use. Enterprises should deploy a well-managed revision control and component repository to prevent poor third-party source code management from compromising existing and future software projects.

Vulnerabilities found in open source frameworks and component libraries are rapidly exploited by hackers as they can automate their attacks knowing that any applications built using the flawed code are vulnerable until a patch is released and installed. Software development teams should have an emergency response plan prepared, to provide a rapid reaction to any critical patch releases for components in use.

MICHAEL COBB, CISSP-ISSAP, is a renowned security author with over 20 years of experience in the IT industry. He co-authored the book IIS Security and has written many technical articles for SearchSecurity.com and other leading IT publications. He was formerly a Microsoft Certified Database Manager and a registered consultant with the CESG Listed Advisor Scheme (CLAS).

Home

Take inventory of your open source software security

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.