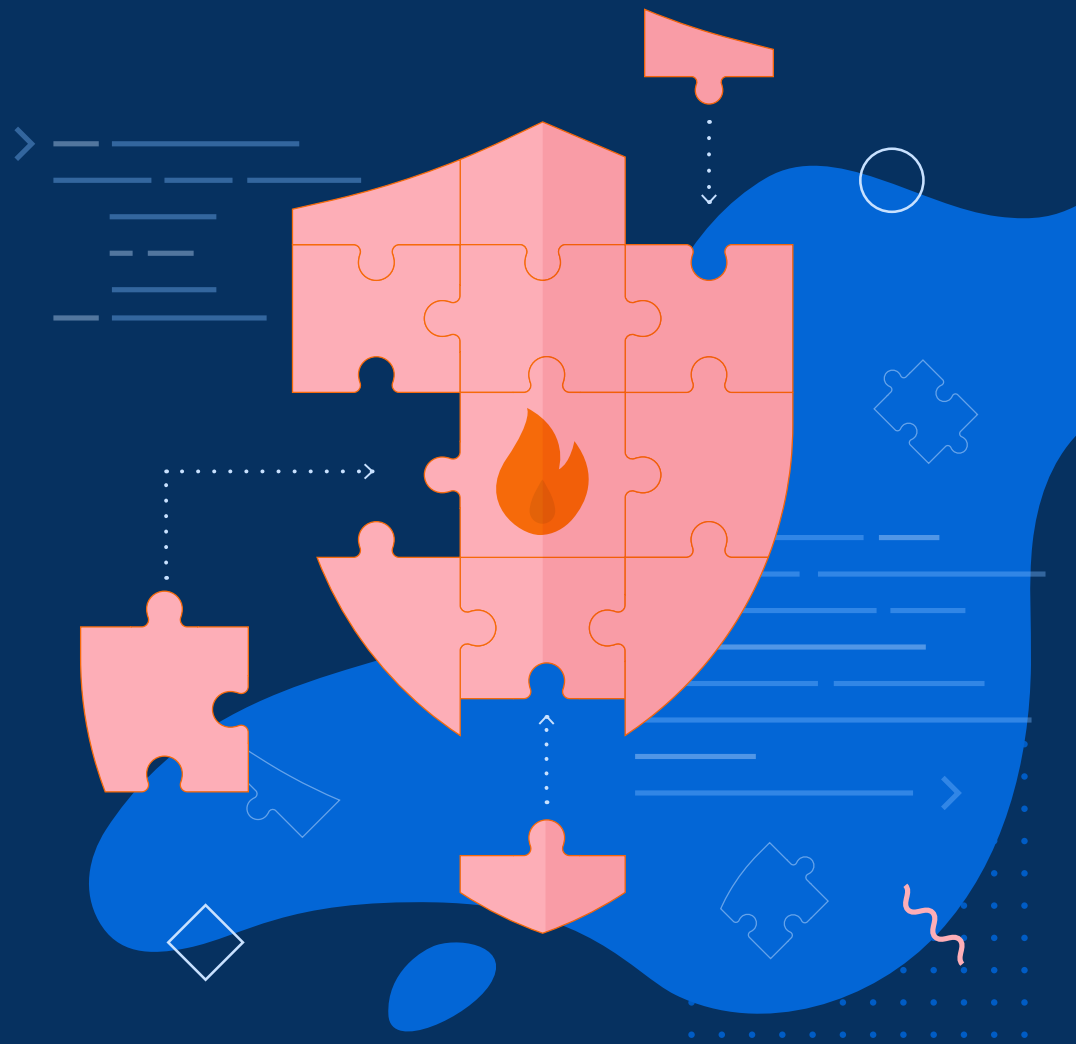
GitHub

How GitHub secures open source software

Learn how GitHub works in public and behind your firewall to protect you as you use, contribute to, and build on open source software.



GitHub's role in securing your open source usage

Open source software is everywhere, powering the languages, frameworks, and applications your team uses every day. **Recent research** has shown that software is now comprised of more than 50 percent open source code. Code available free for everyone to use has changed how software is built—but not without complexity and security concerns. Open source projects can become compromised by outdated libraries and malicious actors, actively trying to subvert them. As you know, these threats expose your organization to additional risk.

At GitHub, we see security as a community problem to solve. By following secure coding practices and diligently fixing vulnerabilities when they are discovered, everyone helps minimize vulnerable targets, making hacking more difficult and less profitable. A safe and healthy open source community isn't just good for open source, it benefits the millions of critical technologies that depend on it. That's why we've built tools and processes that allow organizations to code securely throughout the entire software development lifecycle. Taking security and shifting it to the left allows organizations and projects to prevent code defects that could lead to a vulnerability, before a security incident happens.

GitHub works hard to secure our community and the open source software you use, build on, and contribute to. Through features, services, and security initiatives, we provide the thousands of open source projects on GitHub—and the businesses that rely on them—with best practices to learn and leverage across their workflows. **In 2016**, we raised the industry standard for code review by adding review tools to issues and pull requests. We launched **security alerts** in 2017, token scanning in 2018, and maintainer security advisories and dependency insights in 2019—and we're continuing to iterate and expand on our scope.

Software is now comprised of more than 50 percent open source code.

Making open source more secure

DEPENDENCY VULNERABILITIES

GitHub's dependency vulnerability tools are built in collaboration with the National Vulnerability Database (NVD) to provide in-GitHub alerts for vulnerable libraries—those with outstanding Common Vulnerabilities and Exposures (CVEs)—supporting Ruby, JavaScript, Python, Java, and .NET.

To do so, we take the CVE alerts, which describe vulnerable and remediated versions, then identify them using their respective language dependency management definitions. This allows us to parse a repository's manifests and alert their administrators to vulnerable dependencies and, specifically, to the versions they need to update to, in order to remediate these issues.

Although these capabilities (and more) are currently provided by several third-party tools, our research showed that many open source repositories did not take full advantage of them—and we knew GitHub could help. Since the launch of security alerts, we've sent alerts on more than four million vulnerabilities in open source repositories. So far, we've seen more than 800,000 of these resolved.

Open source repositories on GitHub are more secure than ever.

Beyond NVD data, our platform data also informs our approach to security. Projects can publicize security fixes outside of the NVD in many places, including mailing lists, open source groups, or release notes and changelogs. Regardless of where projects share this information, developers within the GitHub community will see the advisory and immediately bump their required versions of the dependency to a known safe version. When detected, GitHub can use the information in these commits to generate security alerts for vulnerabilities that may not have been published in the CVE feed.

Finding these commits among the vast number Github processes every day requires some machine intelligence. We created a machine learning model to help sift through all commits on dependency files supported by the dependency graph and extract the ones that might be related to a security release. The model uses diffs and commit messages to learn how the required version range changed and understand the intent of the change. Then it aggregates over time to determine if a dependency has released a new version with a security fix that should trigger an alert.

Ensuring open source projects don't rely on libraries that contain vulnerabilities is one way to make an immediate impact.

SOLVING CODE VULNERABILITIES TOGETHER

Ensuring open source projects don't rely on libraries that contain vulnerabilities is one way to make an immediate impact. Another is to help open source projects identify and fix vulnerabilities before they are exposed to the public. We've introduced maintainer security advisories to help the maintainers of open source projects create a private place to collaborate on addressing security vulnerabilities, away from the broader community. This helps maintainers more easily discuss, fix, and publish security advisories to the users that depend on their software without the risk of tipping off would-be hackers.

PROTECTING SECRETS

Even the most secure organizations eventually make a mistake. Just as we've brought vulnerability and dependency security information natively to our platform, we want to help protect developers from leaking secrets as well.

The first step is GitHub Token Scanning—a scalable, real-time code scanning platform that allows us to inspect commits as they are shared with GitHub.com. We launched token scanning with support for platforms including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Slack, and others. For open source repositories, if a developer accidentally commits a credential to any of the supported services, we work with those services to identify the disclosure and proactively invalidate the credentials before anyone uses them in a compromising way.

RESPONSIBLE DISCLOSURE AND ACCESS

Despite code scanning and other secure development practices , vulnerabilities will inevitably be found. And when they are, GitHub makes vulnerability disclosure and management as simple as possible.

To start, we released our Security Advisory API to provide security advisories as a public service. A building block toward a powerful security platform, it provides a way to access the security feeds we aggregate and validate, and the dependency upgrades we monitor across millions of projects. With the API, this data is at your fingertips and ready to be integrated into the tools and workflows you already use.

The Security Advisory API also provides additional capabilities and complements the NVD feeds with concerns like malware and other vulnerabilities that GitHub has found and made available. As a public service, the API provides a foundation for GitHub, researchers, and integrators to collectively create a more secure future.

DEVELOPMENT INSIGHTS

Open source projects are more than just their code. Like any organization, their popularity and impact ebb and flow over time. The most important toolchain today may see its usage drop near zero in just months. GitHub makes it easier for users to understand what's behind the code in each open source project.

With the organization insights dashboard, organizations can have the information they need about the work their teams are doing. The dashboard provides information on patterns of development and utilization of the GitHub platform. Organizations can also track the open source code they currently use. A new second dashboard, the dependency insights dashboard, helps organizations see the open source code their teams depend on and the related vulnerabilities. With visibility to the development languages most prominent in your organization, awareness of security vulnerabilities and resolution, teams are better equipped to make informed decisions and build secure software.

Despite code scanning and other secure development practices, vulnerabilities will inevitably be found.

SECURE CODING

From required reviews to protected branches, GitHub's features help ensure the code committed by your team follows your approved processes and meets strict security standards. And with our Checks-API, developers can access even richer, more actionable status information across testing, vulnerability, and code quality tools.

Along with ensuring the right contributors have access to public projects, GitHub has implemented several ways to validate your users' identities so that only your team is committing code to your projects, including signed commits. GitHub was the first version control platform to support GPG signed commits and now supports for S/MIME X.509 signed commits as of 2018.

We've also added new administrative tools to help control user permissions, run permissions reports, and check audit logs to make sure that your team, and only your team, is accessing your code.

USER SECURITY

GitHub recently improved password and security requirements—and also used public password disclosure databases to invalidate compromised accounts. This continues our history of facilitating proper account hygiene, including two-factor authentication and early FIDO support. We have also recently completed a project to improve the management and permissions of outside collaborators to open source projects. This helps ensure that only the right people from your organization have access to public projects.

PLATFORM HEALTH

To properly protect the code in GitHub projects, we need to make sure the platform itself is secure. Maintaining a software solution that services over 31 million users and thousands of businesses is a large task, especially when there are active efforts by malicious actors to try and cause disruption. In early 2018, GitHub was able to successfully defend against the the largest DDOS attack yet recorded.

To demonstrate our commitment to platform compliance and security, GitHub achieved AICPA Service Organization Controls (SOC) II Type 1 and SOC I Type 1 compliance for GitHub Enterprise Cloud. For international teams using GitHub, we achieved compliance with the IAASB International Standards on Assurance Engagements (ISAE) 3000 and 3402 as well. These two security milestones join our FedRAMP authorization, which allows US government agencies to host their code and securely collaborate on GitHub Enterprise Cloud.

Making your use of open source more secure

As open source gets more secure, so do the apps and software that depend on it. Of course, we'll apply the same tools, features, and products we discussed to your repositories, but we want to help you manage external code as well.

The first piece of this strategy is GitHub Connect: a set of features that brings tighter integration between GitHub Enterprise Cloud, our SaaS-based solution, and GitHub Enterprise Server, our self-hosted solution that can run on-premises, behind your firewall, or in a private cloud. GitHub Connect's three primary features allow you to search for open source code right from your Enterprise Server instance, manage teams, policies, and permissions with a single account, and lastly, help your developers share their skills and contributions at work with the greater open source community.

GITHUB CONNECT

Secure open source is only advantageous if you can easily take advantage of it within your own business. GitHub Connect lets you safely and securely connect to the world's largest community of software developers and open source projects on GitHub.com while maintaining the control and compliance you need from behind the firewall. It also allows us to deliver features and data sourced from the public on GitHub.com to your business environment.

With unified search, developers can search open source and private Enterprise Cloud repositories directly from within GitHub Enterprise. Direct access to these repositories means you can leverage existing projects and better understand what your users are looking for—all within a more managed, visible, and secure workflow.

SECURITY IN THE CLOUD AND ON-PREMISES

Take advantage of GitHub data, including critical security alerts and a clear path to vulnerability mitigation, through GitHub Connect. Developers and organizations are fixing vulnerabilities in their projects, but they don't necessarily notify others. With visibility into the aggregate data behind these fixes, we make sure you aren't using a vulnerable or outdated library—and we alert you if you do.

GitHub Connect eliminates one important choice: staying on-premises or using the cloud.

GETTING THE BEST OF BOTH WORLDS

Finally, as a development leader you know that open source can help your team deliver software, faster, but that doesn't mean risking the security of your users and code. GitHub Connect eliminates one important choice: staying on-premises or using the cloud. Connect to a community of innovation, maximize operational efficiencies, stay more secure, and provide unmatched developer experience—all while keeping your code as close and controlled as you need it to be.

GITHUB AS A PLATFORM

GitHub has always had a best-of-breed philosophy. We're building a platform that allows our partners to create seamless integrations and extend GitHub with new features, functionalities, and workflows. This strategy also holds true for security tools.

We've seen different businesses take different strategies with their security workflows. Some businesses integrate the one tool that best meets their needs, while others integrate multiple tools with the idea that breach prevention is worth any amount of money spent. With the introduction of GitHub Actions, currently in public beta, it's easier than ever to integrate the tools you need.

Whatever your strategy is, you likely don't want to leave security to chance. Being able to integrate tools from leaders in a space, like BlackDuck, HP, IonChannel, LGTM Sonatype, Snyk, and Whitesource, ensures you are able to use the latest applications and services to keep your business secure. And when new tools come along, you can update or replace existing tools as easily as you added them.

If you created in-house tools managing threat intelligence or identifying software vulnerabilities, you can also integrate those into our platform using our APIs (or replace them as necessary). Creating your own alerts within our Advisory database or using our dependency APIs to better understand the libraries and code already in use can help you shift security left—integrating and benefiting from your strategies earlier in your software lifecycle.

Ready to explore securely using Open Source Software at your enterprise?

Contact Us!

sales@github.com

github.com/enterprise

+1 (877) 448-4820