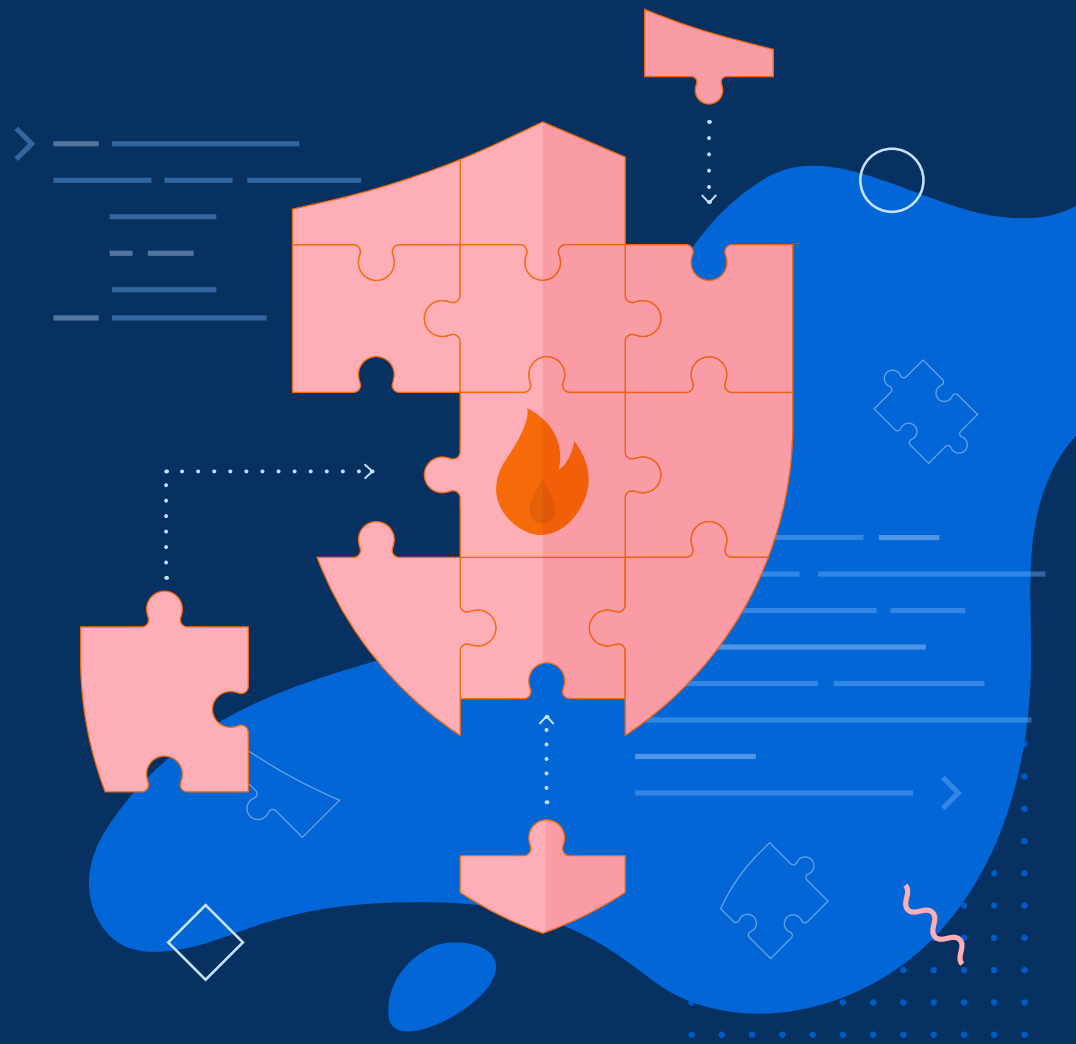
GitHub

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 Open source projects can become compromised by outdated libraries and malicious actors, actively trying to subvert them.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—one that affects all software, regardless of how much proprietary code it contains. Similarly, 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 errors and failures 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 project management and code review by adding GitHub Projects and review tools to issues and pull requests. We believe we can do the same with security. We launched **security alerts** in 2017—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 tools, including Sonatype, Blackduck, and others, 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 vulnerable libraries is one way to make an immediate impact.

CODE VULNERABILITIES

Ensuring open source projects don't rely on vulnerable libraries is one way to make an immediate impact. Another is to help projects build and enforce secure coding practices and prevent security vulnerabilities before they are exposed.

However, 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 accidently 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. We've already **identified millions of potential** tokens during the beta period and look forward to working with even more formats and tools going forward.

Although some of our partners have provided this capability using public GitHub data sources in the past, it will now occur in near-real time (no more 24-hour delays). And with our **Checks-API**, developers can access even richer, more actionable status information across testing, vulnerability, and quality tools.

RESPONSIBLE DISCLOSURE AND ACCESS

Despite code scanning and protection from malicious actors, 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 new 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.

PROJECT 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 Activity Dashboard, organizations can have the insights they need into the work their teams are doing. The Dashboard provides information on patterns of development, utilization of the GitHub platform, and dependency vulnerabilities and issues. 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 more secure software.

Despite code scanning and protection from malicious actors, vulnerabilities will inevitably be found.

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 31 million users and thousands of businesses is a large task, especially when there are active efforts to try and cause disruption, for example the largest DDOS attack yet recorded in early 2018.

Additionally, compliance is an important part of our security work. GitHub is actively engaged in efforts around SOC II compliance, and we have recently received our FedRAMP authorization to securely host code for the U.S. Federal Government.

GENERAL HEALTH

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.

Along with ensuring the right contributors have access to public projects, GitHub has implemented several ways to validate these users' identities, including signed commits. GitHub was the first version control platform to support GPG signed commits and announced support for x509 signed commits in 2018.

Making your use of open source more secure

As open source gets more secure, so does the software that depends 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 first two features bring the power and projects of the open source community to developers using GitHub Enterprise Server. They also provide a unified experience that allows you to better trace users from the open source world to your business.

GITHUB CONNECT

Secure open source is only beneficial 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 keeping your most critical code protected 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 Server. 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 are.

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 have many decisions to make, but GitHub Connect eliminates one important choice: staying on-premises or using the cloud. Connect to a community of innovation, maximize on operational efficiencies, stay more secure, and provide unmatched developer experience—all while keeping your code as close 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 limited 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.

Want more info?

GitHub can help.

Email us at sales@github.com