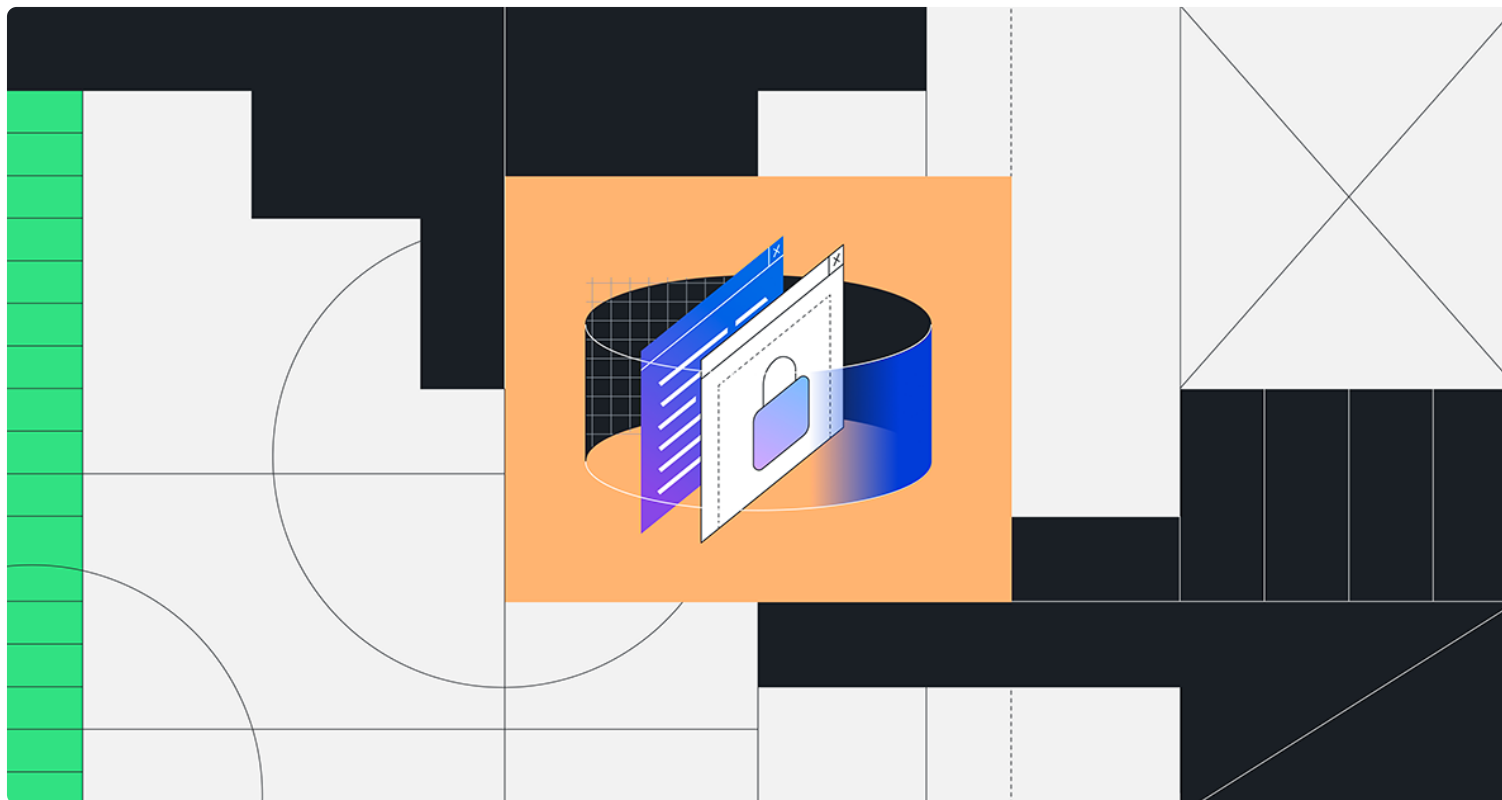


# We updated our RSA SSH host key

At approximately 05:00 UTC on March 24, out of an abundance of caution, we replaced our RSA SSH host key used to secure Git operations for GitHub.com.



Author



**Mike Hanley**

March 23, 2023



At approximately 05:00 UTC on March 24, out of an abundance of caution, we replaced our RSA SSH host key used to secure Git operations for GitHub.com. We did this to protect our users from any chance of an adversary impersonating GitHub or eavesdropping on their Git operations over SSH. This key does not grant access to GitHub's infrastructure or customer data. This change only impacts Git operations over SSH using RSA. Web traffic to GitHub.com and HTTPS Git operations are not affected.

Only GitHub.com's RSA SSH key was replaced. No change is required for ECDSA or Ed25519 users. Our keys are documented [here](#).

## What happened and what actions have we taken?

This week, we discovered that GitHub.com's RSA SSH private key was briefly exposed in a public GitHub repository. We immediately acted to contain the exposure and began investigating to understand the root cause and impact. We have now

completed the key replacement, and users will see the change propagate over the next thirty minutes. Some users may have noticed that the new key was briefly present beginning around 02:30 UTC during preparations for this change.

Please note that this issue was not the result of a compromise of any GitHub systems or customer information. Instead, the exposure was the result of what we believe to be an inadvertent publishing of private information. We have no reason to believe that the exposed key was abused and took this action out of an abundance of caution.

## What you can do

If you are using our ECDSA or Ed25519 keys, you will not notice any change and no action is needed.

If you see the following message when connecting to GitHub.com via SSH, then read onward.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
SHA256:uNiVztkCsDhcc0u9e8BujQXVUpKZIDTMczCvj3tD2s.
Please contact your system administrator.
Add correct host key in ~/.ssh/known_hosts to get rid of this message.
Host key for github.com has changed and you have requested strict checking.
Host key verification failed.
```

If you see the above message, you'll need to remove the old key by running this command:

```
$ ssh-keygen -R github.com
```

Or manually updating your `~/.ssh/known_hosts` file to remove the old entry.

Then, you can manually add the following line to add the new RSA SSH public key entry to your `~/.ssh/known_hosts` file:

```
github.com ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCj7ndNxQowgcQnjshcLrqpEiiphnt+VTTvDP6mHBL9j1aNuK4Ue1gvwnC
```

Or automatically update GitHub.com's RSA SSH key in your `~/.ssh/known_hosts`, by running the following in your terminal:

```
$ ssh-keygen -R github.com
$ curl -L https://api.github.com/meta | jq -r '.ssh_keys | .[]' | sed -e 's/^/github.com /' >> ~/.ssh/known
```

You can verify that your hosts are connecting via our new RSA SSH key by confirming that you see the following fingerprint:

```
SHA256:uNiVztkCsDhcc0u9e8BujQXVUpKZIDTMczCvj3tD2s
```

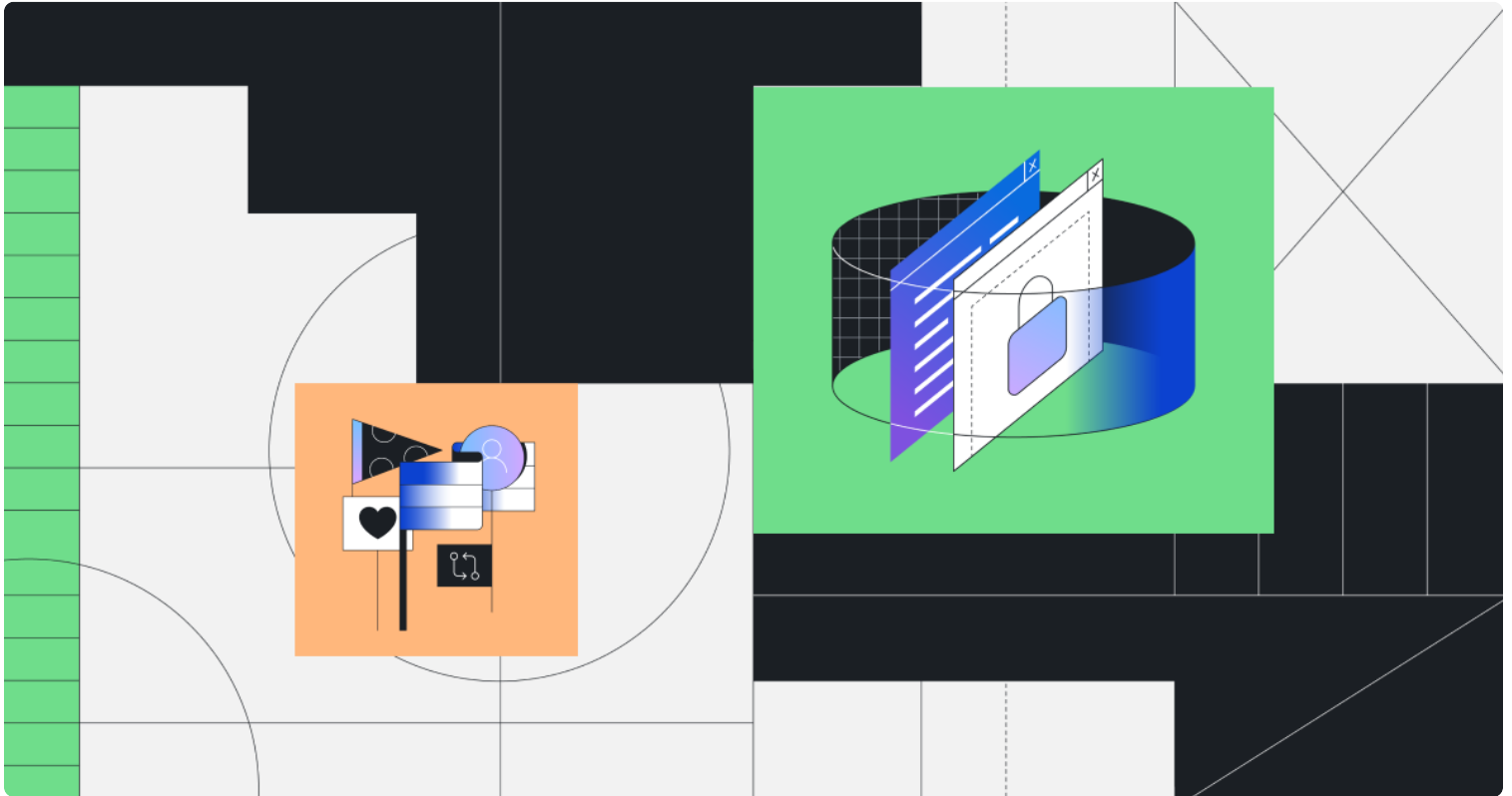
GitHub Actions users may see failed workflow runs if they are using `actions/checkout` with the `ssh-key` option. We are updating the `actions/checkout` action in all our supported tags, including `@v2`, `@v3`, and `@main`. If you pin the action to a

commit SHA and use the `ssh-key` option, you'll need to update your workflow. You can read more about this process [in our official documentation for Actions security hardening](#).

For more information, please visit our [official documentation on GitHub's SSH public key fingerprints](#).

## Related posts

---

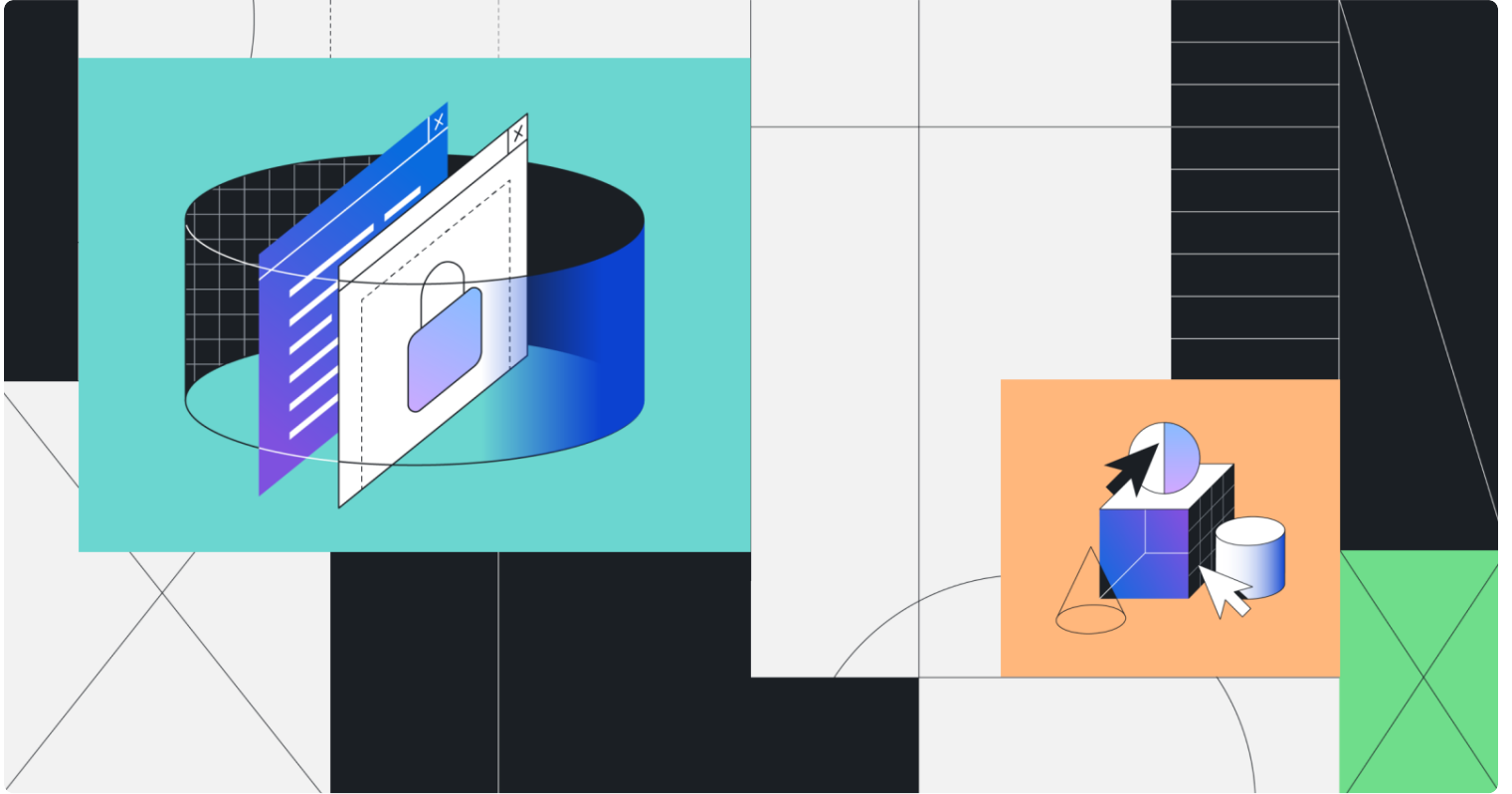


### **Build a secure code mindset with the GitHub Secure Code Game**

Writing secure code is as much of an art as writing functional code, and it is the only way to write quality code. Learn how our Secure Code Game can provide you with hands-on training to spot and fix security issues in your code so that you can build a secure code mindset.

**Joseph Katsioloudes**

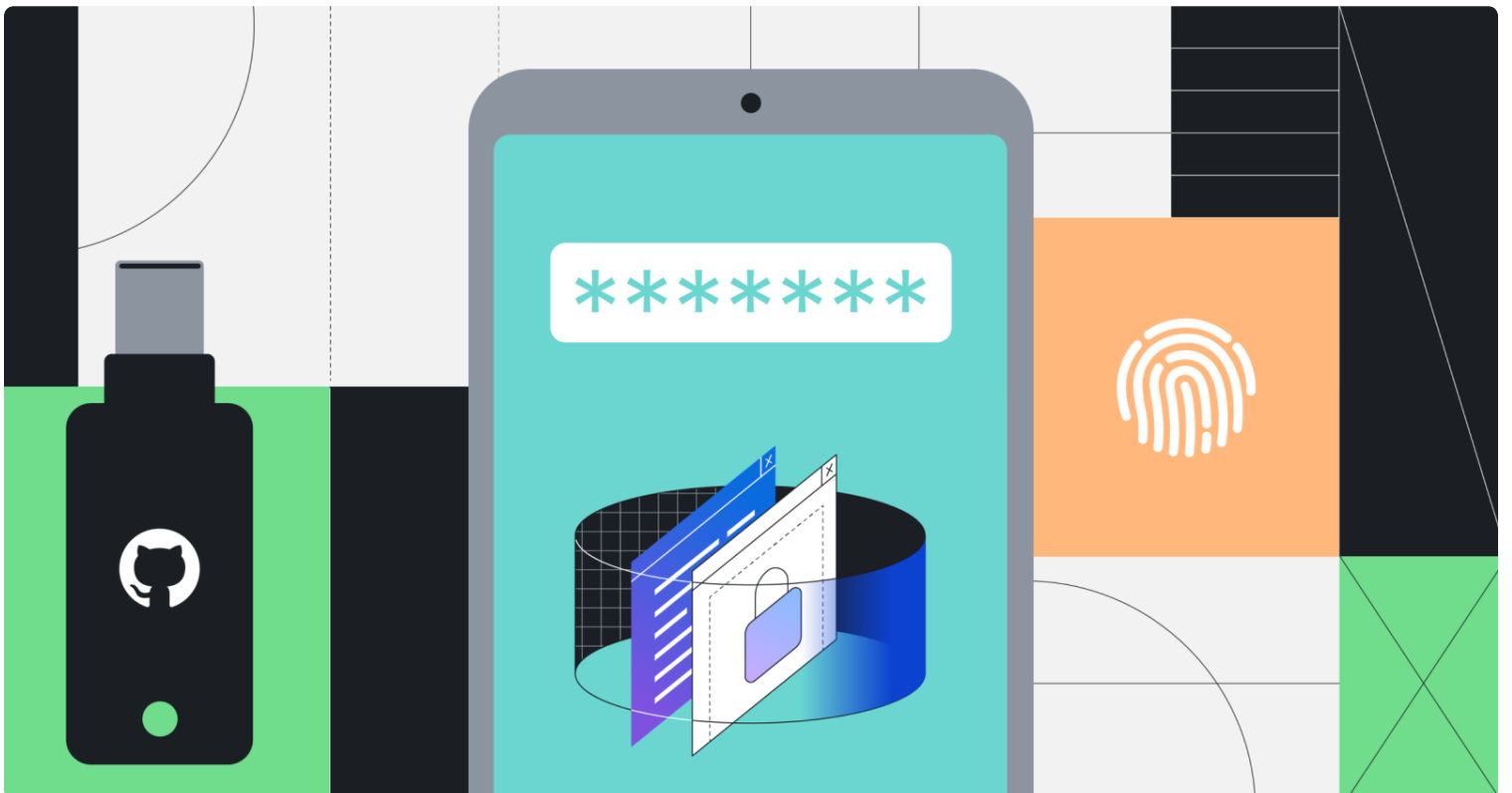
---



## Introducing GitHub vulnerability management integrations for security professionals

Learn about using GitHub Advanced Security alerts with vulnerability management tools. Check out the integrations and learn about how to get started.

Alexander De Michieli & Griffin Ashe



Raising the bar for software security: GitHub 2FA begins March 13

On March 13, we will officially begin rolling out our initiative to require all developers who contribute code on GitHub.com to enable one or more forms of two-factor authentication (2FA) by the end of 2023. Read on to learn about what the process entails and how you can help secure the software supply chain with 2FA.

**Laura Paine & Hirsch Singhal**

## Explore more from GitHub

---

### Security

Secure platform, secure data. Everything you need to make security your #1.

[Learn more >](#)

### Join GitHub Galaxy

Register now for our global enterprise event on March 28–31.

[Register now](#) 


### GitHub Advanced Security

Secure your code without disrupting innovation.

[Learn more](#) 

### Work at GitHub!

Check out our [current job openings](#).

[Learn more](#) 

## Subscribe to The GitHub Insider

A newsletter for developers covering techniques, technical guides, and the latest product innovations coming from GitHub.

Your email address

Yes please, I'd like GitHub and affiliates to use my information for personalized communications, targeted advertising and campaign effectiveness. See the [GitHub Privacy Statement](#) for more details.



Product

Features

Security

Enterprise

Customer Stories

Pricing

Resources

Platform

Developer API

Partners

Atom

Electron

GitHub Desktop

Support

Docs

Community Forum

Training

Status

Contact

Company

About

Blog

Careers

Press

Shop