Secret scanning patterns

Lists of supported secrets and the partners that GitHub works with to prevent fraudulent use of secrets that were committed accidentally.

Secret scanning alerts for partners runs automatically on public repositories and public npm packages to notify service providers about leaked secrets on GitHub.com.
Secret scanning alerts for users are available for free on all public repositories.
Organizations using GitHub Enterprise Cloud with a license for GitHub Advanced Security can also enable secret scanning alerts for users on their private and internal repositories.
For more information, see "About secret scanning" and "About GitHub Advanced Security."

In this article

About secret scanning patterns

GitHub maintains these different sets of default secret scanning patterns:

1. **Partner patterns.** Used to detect potential secrets in all public repositories as well as public npm packages. To find out about our partner program, see "Secret scanning partner program."
2. **User alert patterns.** Used to detect potential secrets in public repositories with secret scanning alerts for users enabled.
3. **Push protection patterns.** Used to detect potential secrets in repositories with secret scanning as a push protection enabled.

Owners of public repositories, as well as organizations using GitHub Enterprise Cloud with GitHub Advanced Security, can enable secret scanning alerts for users on their repositories.

For details about all the supported patterns, see the "Supported secrets" section below.

If you believe that secret scanning should have detected a secret committed to your repository, and it has not, you first need to check that GitHub supports your secret. For more information, refer to the sections below. For more advanced troubleshooting information, see "Troubleshooting secret scanning."

About partner alerts

Partner alerts are alerts that are sent to the secret providers whenever a secret leak is reported for one of their secrets. GitHub currently scans public repositories and public npm packages for secrets issued by specific service providers and alerts the relevant service provider whenever a secret is detected in a commit. For more information about secret scanning alerts for partners, see "About secret scanning."

If access to a resource requires paired credentials, then secret scanning will create an alert only when both parts of the pair are detected in the same file. This ensures that the most critical leaks are not hidden behind information about partial leaks. Pair matching also helps reduce false positives since both elements of a pair must be used together to access the provider's resource.

About user alerts

User alerts are alerts that are reported to users on GitHub. When secret scanning alerts for users are enabled, GitHub scans repositories for secrets issued by a large variety of service providers and generates secret scanning alerts.

You can see these alerts on the **Security** tab of the repository. For more information about secret scanning alerts for users, see "About secret scanning."

If access to a resource requires paired credentials, then secret scanning will create an alert only when both parts of the pair are detected in the same file. This ensures that the most critical leaks are not hidden behind information about partial leaks. Pair matching also helps reduce false positives since both elements of a pair must be used together to access the provider's resource.

If you use the REST API for secret scanning, you can use the `Secret type` to report on secrets from specific issuers. For more information, see "Secret scanning."

About push protection alerts

Push protection alerts are user alerts that are reported by push protection. Secret scanning as a push protection currently scans repositories for secrets issued by some service providers.

Push protection alerts are not created for secrets that are bypassed with user-based push protection only. For more information, see "Push protection for users."

If access to a resource requires paired credentials, then secret scanning will create an alert only when both parts of the pair are detected in the same file. This ensures that the most critical leaks are not hidden behind information about partial leaks. Pair matching also helps reduce false positives since both elements of a pair must be used together to access the provider's resource.

Older versions of certain tokens may not be supported by push protection as these tokens may generate a higher number of false positives than their most recent version. Push protection may also not apply to legacy tokens. For tokens such as Azure Storage Keys, GitHub only supports *recently created* tokens, not tokens that match the legacy patterns. For more information about push protection limitations, see "Troubleshooting secret scanning."

Supported secrets

This table lists the secrets supported by secret scanning. You can see the types of alert that get generated for each token, as well as whether a validity check is

performed on the token.

- **Provider**—name of the token provider.
- **Partner**—token for which leaks are reported to the relevant token partner. Applies to public repositories only.
- **User**—token for which leaks are reported to users on GitHub. Applies to public repositories, and to private repositories where GitHub Advanced Security is enabled.
- **Push protection**—token for which leaks are reported to users on GitHub. Applies to repositories with secret scanning and push protection enabled.
- **Validity check**—token for which a validity check is implemented. Currently only applies to GitHub tokens, and not shown in the table. For more information about validity check support see "Secret scanning patterns" in the GitHub Enterprise Cloud documentation.

Provider	Token	Partner	User	Push protection
Adafruit IO	adafruit_io_key	✓	✓	✓
Adobe	adobe_client_secret	✓	✓	✓
Adobe	adobe_device_token	✓	✓	✓
Adobe	adobe_pac_token	✓	✓	✓
Adobe	adobe_refresh_token	✓	✓	✓
Adobe	adobe_service_token	✓	✓	✓
Adobe	adobe_short_lived_access_token	✓	✓	✓
Aiven	aiven_auth_token	✓	✓	✓
Aiven	aiven_service_password	✓	✓	✓
Alibaba Cloud	alibaba_cloud_access_key_id alibaba_cloud_access_key_secret	✓	✓	✓
Login with Amazon	amazon_oauth_client_id amazon_oauth_client_secret	✓	✓	✓
Amazon Web Services (AWS)	aws_access_key_id aws_secret_access_key	✓	✓	✓
Amazon Web Services (AWS)	aws_session_token aws_temporary_access_key_id	✕	✓	✓

	aws_secret_access_key			
Asana	asana_personal_access_token	✗	✓	✓
Atlassian	atlassian_api_token	✓	✓	✗
Atlassian	atlassian_jwt	✓	✓	✗
Atlassian	bitbucket_server_personal_access_token	✗	✓	✓
Azure	azure_active_directory_application_secret	✓	✓	✓
Azure	azure_batch_key_identifiable	✓	✓	✓
Azure	azure_cache_for_redis_access_key	✗	✓	✓
Azure	azure_container_registry_key_identifiable	✓	✓	✓
Azure	azure_cosmosdb_key_identifiable	✓	✓	✓
Azure	azure_devops_personal_access_token	✓	✓	✓
Azure	azure_function_key	✓	✓	✓
Azure	azure_ml_web_service_classic_identifiable_key	✓	✓	✓
Azure	azure_sas_token	✓	✓	✗
Azure	azure_search_admin_key	✓	✓	✓
Azure	azure_search_query_key	✓	✓	✓
Azure	azure_management_certificate	✓	✓	✗
Azure	azure_sql_connection_string	✓	✓	✗
Azure	azure_sql_password	✓	✓	✓
Azure	azure_storage_account_key	✓	✓	✓

Baidu	baiducloud_api_accesskey	✓	✓	✓
Beamer	beamer_api_key	×	✓	×
Canadian Digital Service	cds_canada_notify_api_key	✓	✓	✓
Checkout.com	checkout_production_secret_key	✓	✓	✓
Checkout.com	checkout_test_secret_key	✓	✓	×
Chief Tools	chief_tools_token	✓	✓	✓
Clojars	clojars_deploy_token	✓	✓	✓
CloudBees CodeShip	codeship_credential	✓	✓	×
Contentful	contentful_personal_access_token	×	✓	×
Contributed Systems	CONTRIBUTED_SYSTEMS_CREDENTIALS	✓	×	×
crates.io (Rust Foundation)	cratesio_api_token	✓	✓	✓
Databricks	databricks_access_token	✓	✓	✓
Datadog	DATADOG_API_KEY	✓	×	×
Defined	defined_networking_nebula_api_key	✓	✓	✓
DevCycle	devcycle_client_api_key	✓	✓	✓
DevCycle	devcycle_mobile_api_key	×	✓	✓
DevCycle	devcycle_server_api_key	✓	✓	✓
DigitalOcean	digitalocean_oauth_token	✓	✓	✓
DigitalOcean	digitalocean_personal_access_token	✓	✓	✓
DigitalOcean	digitalocean_refresh_token	✓	✓	✓
DigitalOcean	digitalocean_system_token	✓	✓	✓

	em_token			
Discord	discord_api_token_v2	✗	✓	✓
Discord	discord_bot_token	✓	✓	✓
Doppler	doppler_audit_token	✓	✓	✓
Doppler	doppler_cli_token	✓	✓	✓
Doppler	doppler_personal_token	✓	✓	✓
Doppler	doppler_scim_token	✓	✓	✓
Doppler	doppler_service_token	✓	✓	✓
Doppler	doppler_service_account_token	✓	✓	✓
Dropbox	dropbox_access_token	✓	✓	✗
Dropbox	dropbox_short_lived_access_token	✓	✓	✓
Duffel	duffel_live_access_token	✗	✓	✓
Duffel	duffel_test_access_token	✗	✓	✗
Dynatrace	dynatrace_access_token	✓	✓	✗
Dynatrace	dynatrace_internal_token	✓	✓	✗
EasyPost	easypost_production_api_key	✗	✓	✓
EasyPost	easypost_test_api_key	✗	✓	✗
eBay	ebay_production_client_id ebay_production_client_secret	✗	✓	✗
eBay	ebay_sandbox_client_id ebay_sandbox_client_secret	✗	✓	✗
Fastly	fastly_api_token	✗	✓	✗
Figma	figma_pat	✓	✓	✓

Finicity	finicity_app_key	✓	✓	×
Flutterwave	flutterwave_live_api_secret_key	×	✓	✓
Flutterwave	flutterwave_test_api_secret_key	×	✓	×
Frame.io	frameio_developer_token	✓	✓	×
Frame.io	frameio_jwt	✓	✓	×
FullStory	fullstory_api_key	✓	✓	✓
GitHub	github_app_installation_access_token	✓	✓	✓
GitHub	github_oauth_access_token	✓	✓	✓
GitHub	github_personal_access_token	✓	✓	✓
GitHub	github_refresh_token	✓	✓	✓
GitHub	github_ssh_private_key	✓	✓	✓
GitLab	gitlab_access_token	×	✓	×
GoCardless	gocardless_live_access_token	✓	✓	×
GoCardless	gocardless_sandbox_access_token	✓	✓	×
Google	firebase_cloud_messaging_server_key	×	✓	×
Google	google_cloud_storage_service_account_access_key_id google_cloud_storage_access_key_secret	×	✓	✓
Google	google_cloud_storage_user_access_key_id google_cloud_storage_access_key_secret	×	✓	✓
Google	google_oauth_access_token	×	✓	×

Google	google_oauth_client_id google_oauth_client_secret	✗	✓	✓
Google	google_oauth_refresh_token	✗	✓	✗
Google Cloud	google_api_key	✓	✓	✗
Google Cloud	google_cloud_private_key_id	✓	✓	✓
Grafana	grafana_cloud_api_key	✓	✓	✓
Grafana	grafana_cloud_api_token	✓	✓	✓
Grafana	grafana_project_api_key	✓	✓	✓
Grafana	grafana_project_service_account_token	✓	✓	✓
HashiCorp	hashicorp_vault_batch_token	✗	✓	✓
HashiCorp	hashicorp_vault_root_service_token	✗	✓	✓
HashiCorp	hashicorp_vault_service_token	✗	✓	✓
Hashicorp Terraform	terraform_api_token	✓	✓	✓
Highnote	highnote_rk_live_key	✓	✓	✓
Highnote	highnote_rk_test_key	✓	✓	✓
Highnote	highnote_sk_live_key	✓	✓	✓
Highnote	highnote_sk_test_key	✓	✓	✓
Hubspot	hubspot_api_key	✓	✓	✓
Hubspot	hubspot_api_personal_access_key	✓	✓	✓
Intercom	intercom_access_token	✗	✓	✓
Ionic	ionic_personal_access_token	✓	✓	✓
Ionic	ionic_refresh_tok	✓	✓	✓

	en			
JD Cloud	jd_cloud_access_key	✓	✓	×
JFrog	jfrog_platform_access_token	×	✓	✓
JFrog	jfrog_platform_api_key	×	✓	✓
JFrog	jfrog_platform_reference_token	×	✓	✓
Linear	linear_api_key	✓	✓	✓
Linear	linear_oauth_access_token	✓	✓	✓
Lob	lob_live_api_key	×	✓	×
Lob	lob_test_api_key	×	✓	×
LocalStack	localstack_api_key	✓	✓	×
LogicMonitor	logicmonitor_bearer_token	✓	✓	✓
LogicMonitor	logicmonitor_lmv1_access_key	✓	✓	✓
Mailchimp	mailchimp_api_key	✓	✓	×
Mailchimp	MANDRILL_API	✓	×	×
Mailgun	mailgun_api_key	✓	✓	×
Mapbox	mapbox_secret_access_token	×	✓	×
Maxmind	maxmind_license_key	✓	✓	✓
Mercury	mercury_non_production_api_token	×	✓	×
Mercury	mercury_production_api_token	×	✓	×
MessageBird	messagebird_api_key	✓	✓	×
Meta	facebook_access_token	✓	✓	×
Midtrans	midtrans_production_server_key	×	✓	✓
Midtrans	midtrans_sandbox_server_key	×	✓	×

New Relic	new_relic_insights_query_key	✗	✓	✓
New Relic	new_relic_license_key	✗	✓	✗
New Relic	new_relic_personal_api_key	✗	✓	✓
New Relic	new_relic_rest_api_key	✗	✓	✓
Notion	notion_integration_token	✗	✓	✗
Notion	notion_oauth_client_secret	✗	✓	✗
npm	npm_access_token	✓	✓	✓
NuGet	nuget_api_key	✓	✓	✓
Octopus Deploy	octopus_deploy_api_key	✓	✓	✗
Oculus	oculus_very_tiny_encrypted_session	✗	✓	✗
OneChronos	onechronos_api_key	✗	✓	✓
OneChronos	onechronos_eb_api_key	✗	✓	✓
OneChronos	onechronos_eb_encryption_key	✗	✓	✓
OneChronos	onechronos_oauth_token	✗	✓	✓
OneChronos	onechronos_refresh_token	✗	✓	✓
Onfido	onfido_live_api_token	✓	✓	✓
Onfido	onfido_sandbox_api_token	✓	✓	✗
OpenAI	openai_api_key	✓	✓	✓
OpenAI	openai_api_key_v2	✓	✓	✓
Palantir	palantir_jwt	✓	✓	✓
Persona	persona_production_api_key	✗	✓	✗
Persona	persona_sandbo	✗	✓	✗

	x_api_key			
Pinterest	pinterest_access_token	✓	✓	✓
Pinterest	pinterest_refresh_token	✓	✓	✓
PlanetScale	planetscale_database_password	✓	✓	✓
PlanetScale	planetscale_oauth_token	✓	✓	✓
PlanetScale	planetscale_service_token	✓	✓	✓
Plivo	plivo_auth_id plivo_auth_token	✓	✓	✓
Postman	postman_api_key	✓	✓	✓
Postman	postman_collection_key	✕	✓	✓
Prefect	prefect_server_api_key	✓	✓	✓
Prefect	prefect_user_api_key	✕	✓	✓
Prefect	PREFECT_USER_API_TOKEN	✓	✕	✕
Proctorio	proctorio_consumer_key	✓	✓	✕
Proctorio	proctorio_linkage_key	✓	✓	✕
Proctorio	proctorio_registration_key	✓	✓	✕
Proctorio	proctorio_secret_key	✓	✓	✓
Pulumi	pulumi_access_token	✓	✓	✕
PyPI	pypi_api_token	✓	✓	✕
ReadMe	readmeio_api_access_token	✓	✓	✓
redirect.pizza	redirect_pizza_api_token	✓	✓	✓
Rhosys	authress_service_client_access_key	✕	✓	✓
Rootly	rootly_api_key	✓	✓	✓

RubyGems	rubygems_api_key	✓	✓	✗
Samsara	samsara_api_token	✓	✓	✓
Samsara	samsara_oauth_access_token	✓	✓	✓
Segment	segment_public_api_token	✓	✓	✓
SendGrid	sendgrid_api_key	✓	✓	✓
Sendinblue	sendinblue_api_key	✓	✓	✓
Sendinblue	sendinblue_smtp_key	✓	✓	✓
Shippo	shippo_live_api_token	✗	✓	✓
Shippo	shippo_test_api_token	✗	✓	✗
Shopify	shopify_access_token	✓	✓	✓
Shopify	shopify_app_client_credentials	✗	✓	✗
Shopify	shopify_app_client_secret	✗	✓	✗
Shopify	shopify_app_shared_secret	✓	✓	✓
Shopify	shopify_custom_app_access_token	✓	✓	✗
Shopify	shopify_marketplace_token	✗	✓	✗
Shopify	shopify_merchant_token	✗	✓	✗
Shopify	shopify_partner_api_token	✗	✓	✗
Shopify	shopify_private_app_password	✓	✓	✗
Slack	slack_api_token	✓	✓	✓
Slack	slack_incoming_webhook_url	✓	✓	✗
Slack	slack_workflow_webhook_url	✓	✓	✗
Square	square_access_t	✗	✓	✗

	oken			
Square	square_production_application_secret	✗	✓	✗
Square	square_sandbox_application_secret	✗	✓	✗
SSLMate	sslmate_api_key	✓	✓	✗
SSLMate	sslmate_cluster_secret	✓	✓	✗
Stripe	stripe_live_restricted_key	✓	✓	✗
Stripe	stripe_api_key	✓	✓	✓
Stripe	stripe_legacy_api_key	✓	✓	✗
Stripe	stripe_test_restricted_key	✓	✓	✗
Stripe	stripe_test_secret_key	✓	✓	✗
Stripe	stripe_webhook_signing_secret	✗	✓	✗
Supabase	supabase_service_key	✓	✓	✗
Tableau	tableau_personal_access_token	✗	✓	✗
Telegram	telegram_bot_token	✗	✓	✗
Telnyx	telnyx_api_v2_key	✓	✓	✓
Tencent Cloud	tencent_cloud_secret_id	✓	✓	✓
Tencent WeChat	tencent_wechat_api_app_id	✓	✓	✗
Twilio	twilio_access_token	✗	✓	✓
Twilio	twilio_account_sid	✓	✓	✓
Twilio	twilio_api_key	✓	✓	✓
Typeform	typeform_personal_access_token	✓	✓	✓
Uniwise	wiseflow_api_key	✓	✓	✓
WakaTime	wakatime_pp_se	✓	✓	✓

WakaTime	wakatime_pp_secret	✓	✓	✓
WakaTime	wakatime_oauth_access_token	✓	✓	✓
WakaTime	wakatime_oauth_refresh_token	✓	✓	✓
Workato	workato_developer_api_token	✓	✓	✓
WorkOS	workos_production_api_key	✗	✓	✓
WorkOS	workos_staging_api_key	✗	✓	✗
Yandex	yandex_iam_access_secret	✓	✓	✗
Yandex	yandex_cloud_api_key	✓	✓	✗
Yandex	yandex_cloud_iam_cookie	✓	✓	✗
Yandex	yandex_cloud_iam_token	✓	✓	✗
Yandex	yandex_cloud_smartcaptcha_server_key	✗	✓	✓
Yandex	yandex_dictionary_api_key	✗	✓	✗
Yandex	YANDEX_PASSPORT_OAUTH_TOKEN	✓	✗	✗
Yandex	yandex_predictor_api_key	✗	✓	✗
Yandex	yandex_translate_api_key	✗	✓	✗
Zuplo	zuplo_consumer_api_key	✓	✓	✓

Further reading

- "Securing your repository"
- "Keeping your account and data secure"
- "Secret scanning partner program"