GitGuardian Unveils "HasMySecretLeaked," Bringing Leak Detection to Every Secret In The DevOps Pipeline

The company's latest project helps organizations proactively check if their developer secrets and credentials have leaked in public.

BOSTON, MA, UNITED STATES, October 17, 2023 /EINPresswire.com/ -- GitGuardian, the leading software supply chain security platform, unveils 'HasMySecretLeaked,' a free toolset to help security engineers proactively verify if their organization's secrets have leaked on GitHub.com.

Ensuring Secrets Remain Safe: A Critical Challenge

Securing secrets is a daunting task in the cloud-native application development world. Organizations grapple with secrets sprawl, where API keys and database credentials proliferate across developer tools. Furthermore, secrets are susceptible to leaks during "out of office hours," often in assets beyond an organization's control, namely personal GitHub repositories, Docker images, or open-source packages.

In response, GitGuardian presents 'HasMySecretLeaked,' a private database with over 20 million records of hashed secrets leaked in public sources, including GitHub.com. Users can query the database by submitting a hashed version of their secret in the search console, and GitGuardian will look for their perfect matches–without revealing any other secrets or their locations.

"Knowing whether your 'vaulted' secrets have leaked publicly is just one API call away. We built a privacy-safe and secure process that returns an unequivocal answer to the crucial question: Has my secret leaked?" said Eric Fourrier, co-founder and CEO of GitGuardian.

Enabling Security And Development Teams To Verify Every Secret

Since 2017, GitGuardian has assisted application security, platform engineering, and development teams in reducing their organizations' attack surface by remediating exposed secrets. With 'HasMySecretLeaked', however, GitGuardian is elevating secrets security in new ways, bringing systematic leak checks to every secret in the DevOps pipeline.

Also, starting today, GitGuardian users can harness the power of 'HasMySecretLeaked' directly from the command-line interface ggshield. In addition, ggshield includes plug-ins for pulling

secrets from popular tools like HashiCorp Vault and AWS Secrets Manager and staging them in local environments before leak inspection.

The capability is also already integrated into the GitGuardian Platform. It will notify security teams if their hardcoded secrets, found in organization-owned repositories, Slack workspaces, or Jira projects, are unintentionally leaked to public sources the organization cannot control or see.

“It’s more than just visibility. Undetected public exposure makes all the difference between a simple alert and a critical incident. It’s the context security teams badly need to prioritize remediation,” said Edouard Viot, Vice President of Product at GitGuardian.

A Unique Database Powered by Unrivaled Engineering

GitGuardian scans every public commit on GitHub for leaks, spanning API keys, database assignments, and developer secrets. In 2020, it uncovered 3 million exposed secrets, surging to 6 million in 2021 and an astounding 10 million in 2022. GitGuardian’s monitoring capabilities position ‘HasMySecretLeaked’ as a one-of-a-kind solution for organizations seeking to audit the security of their secrets.

GitGuardian also understands the importance of protecting secrets from unwanted exposure and has designed HasMySecretLeaked in a way that does not read or access users’ secrets.

“We’re leveraging concepts such as k-anonymity and zero-knowledge, making it impossible for us or anyone else to see or reconstruct the secrets, all while determining whether they have leaked in public sources,” said Eric Fourrier.

Visit the official website to try HasMySecretLeaked or book a demo with GitGuardian.
This article gives more details about the underlying protocol

About GitGuardian

GitGuardian, founded in 2017, has become the leader in automated secrets detection and is now focused on providing a comprehensive software supply chain security platform. It's raised $56M from top investors, including co-founders of GitHub and Docker. Its policy engine helps security teams monitor and enforce rules across all their VCS, DevOps tools, and infrastructure-as-code configurations.

GitGuardian offers Secrets Detection, Infra as Code Security, and Honeytoken capabilities all in one platform. It helps software-driven organizations strengthen their overall security posture and comply with application security frameworks and standards. Its secrets detection engine is trained against over a billion public GitHub commits annually, covering 350+ types of secrets. The platform brings security and development teams together with automated remediation

playbooks and collaboration features to achieve shorter fix times.

GitGuardian is trusted by leading companies, including Instacart, Snowflake, Orange, Bouygues Telecom, Iress, Maven Wave, NOW: Pensions, DataDog, and PayFit. Used by more than 300K developers, it ranks #1 in the security category on GitHub Marketplace."

Please visit the official website to learn more.

Holly Hagerman
Connect Marketing for GitGuardian
+1 801-373-7888
hollyh@connectmarketing.com
