Key Learnings from the Disney Breach: 5 Ways to Stop Secret Sprawl | Nightfall AI

By Puja Shah

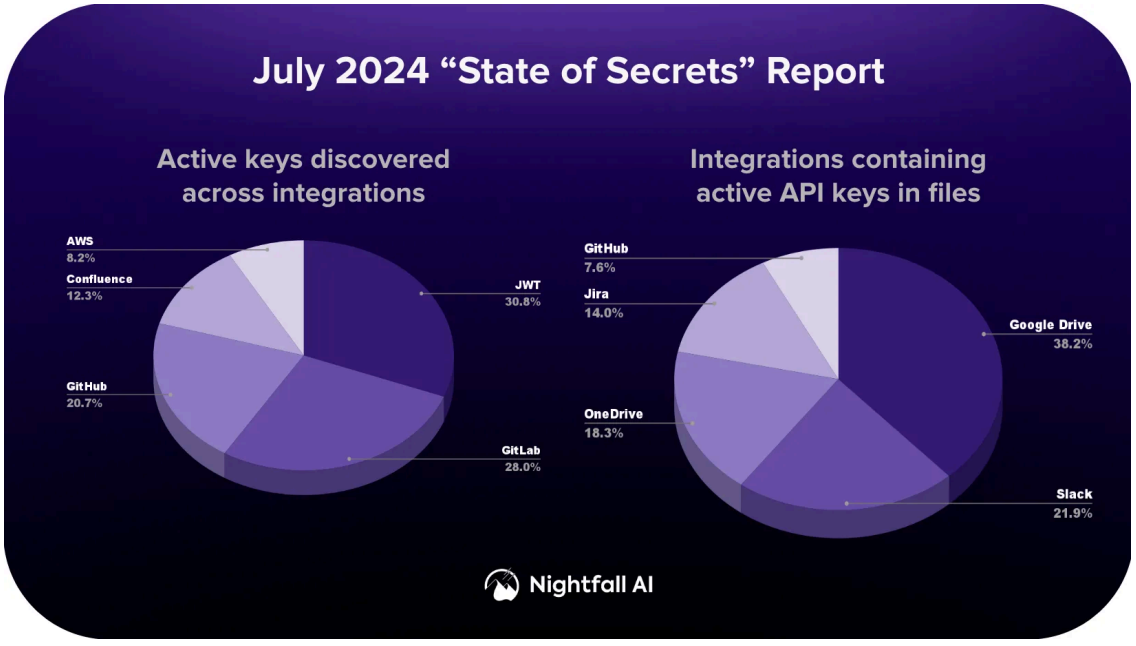
Archived: 2026-04-05 16:46:21 UTC

Do you have secrets sprawled across your tech stack? The recent Disney breach is as good a reminder as any to check, because it's likely that you do. But first, let's take a closer look at the Disney breach to understand what may have gone wrong, and how you can prevent a similar breach from happening to your business.

What caused the Disney breach?

According to CSO Online, a hacker group leaked "one terabyte of data from Disney's Slack channels, which include[s] computer code and information on unreleased projects." The data also contains "discussions on managing Disney's corporate website, software development, and job applicant evaluations," as reported by the Wall Street Journal.

While the exact cause of the breach has yet to be confirmed, some are speculating that it could easily have been caused by a sprawled Slack API key. Due to the interconnected nature of today's enterprise workplaces, it's increasingly common for API keys, passwords, and other secrets to be shared in messages, files, and screenshots. Each of these shared API keys present an opportunity for threat actors who are looking to escalate their privileges and access even more valuable company and customer data.



How common is secret sprawl?

The Disney breach is just one among many recent breaches that involve secret sprawl. For instance, the Sisense breach earlier this year was caused by a sprawled AWS S3 credential in GitLab, and the Okta breach late last year was caused by a stolen credential that granted access to session tokens in customer HAR files.

These past breaches only go to show that secret sprawl is far more prevalent than you think. At Nightfall, we've detected over 3 million secrets that have been sprawled across apps like Slack, GitHub, and Jira, just to name a few. We've also found that for every 100 employees, there's an average of 5 active API keys leaked across the cloud. As we've now seen with Disney, this sort of unchecked secret sprawl can widen the impact and severity of a breach, leading to steeper financial and legal costs, as well as the loss of customer and stakeholder trust.

What are best practices to prevent secret sprawl?

By containing secret sprawl, organizations can prevent unauthorized data access and strengthen their overall security posture. Read on for Nightfall's top five strategies for safeguarding secrets, and, by extension, staving off data breaches.

1. **Scan for sprawled secrets:** It's important to have visibility into the places where secrets are shared across SaaS and GenAI apps, both historically and in real time. Automated data leak prevention (DLP) tools can be useful for pinpointing and quickly addressing any instances where secrets might be exposed or mismanaged.

2. **Automatically remediate secrets:** Set up real-time notifications and automated workflows to delete, redact, rotate, or encrypt secrets the instant they're shared. Automation can speed up time to remediation, which helps to stop secret sprawl at the source, before it can proliferate across the cloud.

3. **Rotate API keys regularly:** Establish a regular schedule for rotating API keys and develop a clear process for updating and distributing new keys to ensure all systems and applications are synchronized with the latest credentials. These practices will mitigate the risk of compromised credentials and protect against unauthorized data access.

4. **Coach employees about secret sharing best practices:** Data sprawl is, more often than not, completely unintentional. It's important to help employees to understand where and how it's appropriate to share secrets for business-critical workflows. While these processes may be covered during onboarding or annual security training, it's a good idea to implement real-time notifications and coaching in order to maintain awareness of security policies year round.

5. **Encrypt secrets before you share them:** If you must share secrets with coworkers, ensure that they're shared safely, either via encrypted communications or via password managers. For highly sensitive information, consider using an end-to-end encryption solution that can detect sensitive data and automatically encrypt it before it leaves the client side.

By implementing the above best practices, you can significantly reduce the risk of secret sprawl and improve overall security posture within your organization.

TL;DR

The Disney breach underscores the critical need for effective secret management to prevent privilege escalation attacks and data breaches. Nightfall's comprehensive, AI-powered DLP platform offers a robust solution to this challenge by:

- Monitoring for secret sprawl both in real time and historically across SaaS and GenAI apps as well as email and endpoints
- Automatically encrypting secrets to help teams share share business-critical data safely
- Sending automated notifications to educate employees when they violate a secret-sharing policy, and ask them to self-remediate the issue

Learn more about how you can address secret sprawl by scheduling a custom demo with our team, or by signing up for our free Firewall for AI platform today.
