Google Workspace security vulnerability caused thousands of user accounts to be attacked

Google Workspace is a service that allows businesses to create professional email addresses using their company domain name.

While the world is still reeling from the CrowdStrike incident, another major work support software service platform, Google Workspace, also recently faced a serious security issue related to user accounts. use.

Google Workspace is a service that allows businesses to create professional email addresses using their company domain name, such as abc@tencongty.com. Additionally, businesses can also access Google Drive, Gmail calendar, Google Meet, etc. through a Google Workspace account.

Google's security team recently discovered that hackers were able to bypass the email verification system, which is required to create a Google Workspace account. For example, if you want to create a Google Workspace account for abc@tencongty.com, you first need to verify that the email address belongs to you. However, hackers have found a trick to bypass this basic requirement. Worse, the created Google Workspace account can be used at third-party services that allow "Sign in with Google" as a sign-in mechanism.

Here's how hackers bypass email verification for Google Workspace accounts:

1. Google offers a free Workspace trial account that allows users to try out services like Google Docs.
2. However, to create a Workspace account with Gmail and domain-dependent services, email verification is required.
3. Hackers created a request specifically crafted to avoid email verification during the registration process.
4. Hackers will use one email address to attempt login and a completely different email address to verify the token.

5. After verifying the email, in some cases, hackers can access third-party services using Google's single sign-on feature.

Google informed KrebsOnSecurity that the issue began in late June, affecting "several thousand" Workspace accounts, and that it successfully fixed the issue within 72 hours of discovery. The company also confirmed that it has added detection features to protect against these types of authentication bypasses.

However, according to reports from some users, it seems that the email verification bypass issue has been going on for more than a month. There was one case of users being affected by this issue on June 6, which was not the end of the month as Google claimed. Another user on the KrebsOnSecurity forum named David Keaton claimed to have encountered an issue with Google on June 7.

Google's lack of transparency about the timeline and full extent of the Workspace security vulnerability raises concerns. A clear and detailed public announcement, including proactive steps taken to prevent future violations, would be a more responsible approach. Additionally, acknowledging the issue with an official blog post would help Google demonstrate the company's commitment to transparency and user trust.