Google Cloud Platform Vulnerability Led to Stealthy Account Backdoors



A vulnerability in Google Cloud Platform (GCP) could have allowed attackers to maliciously change an OAuth application and hide it to create a stealthy backdoor to any Google account.

Exploitation of the bug, referred to as GhostToken, could have allowed attackers to completely hide the malicious application from the Google user and leverage it to retrieve account tokens to access the victim's data.

The issue was related to the deletion of OAuth clients, which essentially are GCP projects, app-to-app security firm Astrix, which identified the flaw in June last year, explains.

When a GCP project is deleted – either by the owner or anyone that has the necessary management permissions – the project enters a 'pending deletion' state for 30 days, allowing the

developer to restore it if necessary.

However, when they are deleted, they are no longer displayed in the Google account application management page, even if they continue to have access to the account.

The same applies to GCP projects that are OAuth clients. While the user receives an error informing them that the client had been deleted, the application continues to have access to the account until effectively deleted.

Astrix also discovered that, when such an OAuth client is restored from the ‘pending deletion’ state, the refresh token created when the user first authorized the application is re-enabled.

This refresh token, the security firm explains, can then be used to get an access token to the victim’s account, and then access their data.

To exploit this vulnerability, an attacker could create or take over an OAuth application, thus gaining access to the refresh token. The attacker could then delete the project associated with the app to prevent the victim from removing it from their account.

Whenever the attacker wanted to access the victim’s data, they would restore the project, use the refresh token to get an access token, and then delete the project again to hide the application and make it unremovable.

“By exploiting the GhostToken vulnerability, attackers can hide their malicious application from the victim’s Google account application management page. Since this is the only place Google users can see their applications and revoke their access, the exploit makes the malicious app unremovable from the Google account,” Astrix notes.

In this scenario, the access token would allow the attacker to

read the victim’s emails, access their Google Drive and Photos files, view their calendar, track their location, and “grant access to the victim’s Google Cloud Platform services”, the security firm explains.

In April 2023, Google addressed the vulnerability by making applications that are in a ‘pending deletion’ state visible in the Google account, so that users can remove them.

Related: Google Wants Android Users to Have More Control Over Their Data

Related: Google Suspends Chinese Shopping App Amid Security Concerns

Related: Google Workspace Client-Side Encryption Now Generally Available in Gmail, Calendar

Google Cloud Platform Vulnerability Led to Stealthy Account Backdoors