Exploring a Critical Risk in Google Workspace's Domain-Wide Delegation Feature

By Zohar Zigdon

Published: 2023-11-30 · Archived: 2026-04-05 15:00:18 UTC

Executive Summary

Unit 42 researchers discovered a security risk in the Google Workspace (formerly known as G Suite) domain-wide delegation feature. We exposed an unexpected way to gain access to the Google Workspace domain data from Google Cloud Platform (GCP).

We found that a GCP identity with the necessary permission can generate an access token to a delegated user. A malicious insider or an external attacker with stolen credentials can use this access token to impersonate Google Workspace users, granting unauthorized access to their data or to perform operations on their behalf.

In this article, we will highlight the risk of the Google Workspace domain-wide delegation feature. In doing so, we will explore its potential misuse by malicious actors and examine the implications for the security of Google Workspace data.

As organizations increasingly rely on the power of cloud-based services like Google Workspace and Google Cloud Platform GCP, it becomes crucial to delve into the intricacies of their security features and vulnerabilities. We will discuss the link between GCP and Google Workspace and examine how the GCP permission model can impact the security of Google Workspace.

Palo Alto Networks customers receive protection from the issue discussed in this article through Cortex XDR and Prisma Cloud.

Domain-Wide Delegation Misuse Overview

Simulation

A possible attack path shown in Figure 1 could be a malicious insider (e.g., a developer with editor permissions in a GCP project) exploiting their access. They could do so by abusing a service account that is granted domain-wide delegation permissions in Google Workspace. The insider has permission to generate access tokens to service accounts within the same GCP project.

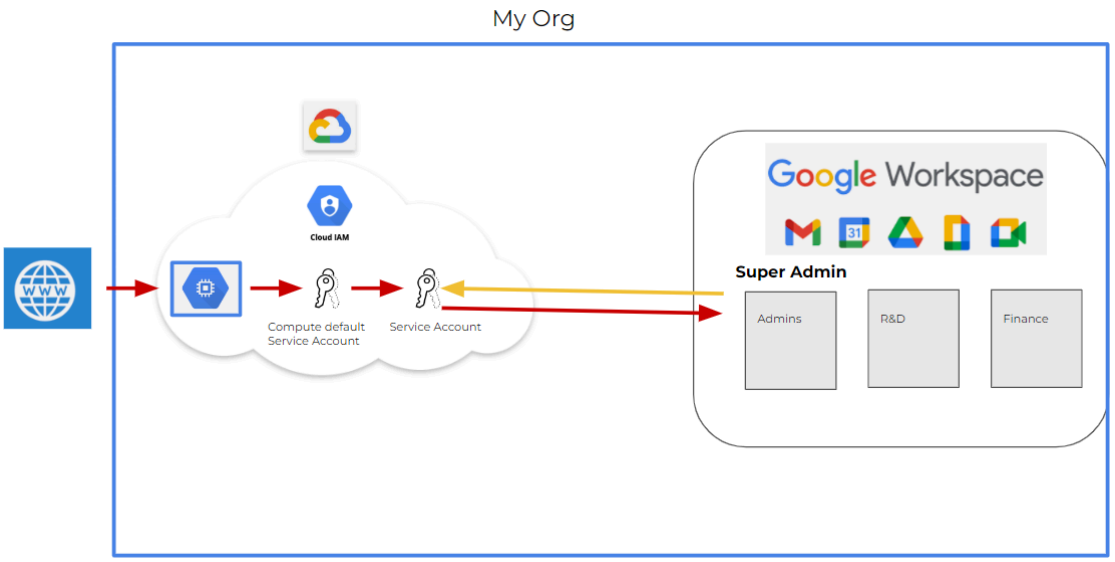

Figure 1. Second attack scenario.

With the domain-wide delegation permissions enabled, a malicious insider can impersonate users in the Google Workspace domain and use the access tokens to authenticate API requests. By leveraging the appropriate scopes and API access, the insider can access and retrieve sensitive Google Workspace data, potentially compromising emails, documents and other confidential information stored within the domain. Such actions highlight the threats of the domain-wide delegation feature.

A worst case scenario would come about if an attacker has obtained a GCP service account token attached to a compute engine instance (e.g., the compute engine default service account, which has editor permissions by default). From there, the attacker may be able to exploit the domain-wide delegation feature for larger impact. If in the same project, a service account with domain-wide delegation exists, this can lead the attacker to impersonate the delegated service account and move laterally from GCP to gain access to the Google Workspace environment.

Google Workspace

Before we delve into the intricacies of a recent security risk that surfaced within Google Workspace and GCP, it is crucial to establish a solid foundation of understanding about these powerful cloud-based services.

Google Workspace apps are a collection of cloud-based collaboration tools. Organizations use Google Workspace to enhance their productivity and communication through various tools such as the following:

- Email
- Calendar
- File storage and sharing
- Team communication
- Workflow automation
- Security
- Administration

Google Workspace provides role-based access control (RBAC) capabilities and allows administrators to assign specific roles to users, granting them predefined sets of permissions based on their responsibilities and needs. These roles include the following:

- Super admin
- Groups admin
- User management admin

Each role has specific privileges and controls over different aspects of the organization's Google Workspace environment. The Google Workspace super admin holds elevated permissions and broader domain management responsibilities, including the ability to grant domain-wide delegation permission to service accounts, which we will explore in more detail later.

Google Workspace administrators can also define application-specific permissions and restrict sharing and visibility settings. For example, an administrator can enforce policies that prevent users from publicly sharing files and limit sharing options to ensure files remain within authorized boundaries.

A common use case for a link between GCP and Google Workspace is when an application hosted on GCP needs to interact with one of the Google Workspace services. These services include the following:

- Gmail
- Calendar
- Drive
- Docs

This integration allows the application to access and manipulate user-specific data, perform actions on behalf of users, or leverage the collaboration and productivity features of Google Workspace.

A delegated GCP service account is required to create an application that interacts with Google services, accesses Google APIs, handles users' data or performs actions on their behalf.

What Is a Service Account?

A service account is a special type of account in GCP that represents nonhuman entities, such as applications or virtual machines. It allows them to authenticate and interact with Google APIs. A service account is associated with the application itself rather than an individual end user.

Service accounts are not members of your Google Workspace domain, unlike user accounts. They aren't subject to domain policies set by Google Workspace administrators and can only access users' data if they are granted domain-wide delegation.

What Is Domain-Wide Delegation?

Domain-wide delegation is a feature in Google Workspace that allows GCP service accounts to access Google Workspace users' data and to act on their behalf within a specific domain.

When using the domain-wide delegation feature, applications can act on behalf of users in a Google Workspace domain without requiring individual users to authenticate and authorize the application.

Only a Google Workspace super admin can authorize an application, acting as the service account, to access data on behalf of users in a domain. This authorization is called “delegating domain-wide authority" to a service account.

How Does Domain-Wide Delegation Work?

To use the domain-wide delegation feature, the following steps (shown in Figure 2) are required:

1. Enabling Domain-Wide Delegation: The Google Workspace super admin grants domain-wide delegation for a service account, along with a set of OAuth scopes allowed for that access. These scopes detail which specific services and specific actions the service account will have access to. For example, if just the scope /auth/gmail.readonly is granted, the service account will have access to read a user’s Gmail messages when acting on behalf of that user, but not their other Workspace data such as access to files in Drive.
2. Requesting Google Workspace Access Token: The application sends a request to the Google Workspace token endpoint with the appropriate credentials. This includes the service account's client ID and client secret, as well as the desired scopes for accessing the user data. If the request is valid and the service account has been granted the necessary domain-wide delegation privileges, the token endpoint responds with an access token. The application can use this access token to access user data across the domain within the limits of the scopes requested.
3. API Access: The application includes the access token in API requests as an authorization header, and it acts as proof of authentication and authorization on behalf of the service account.

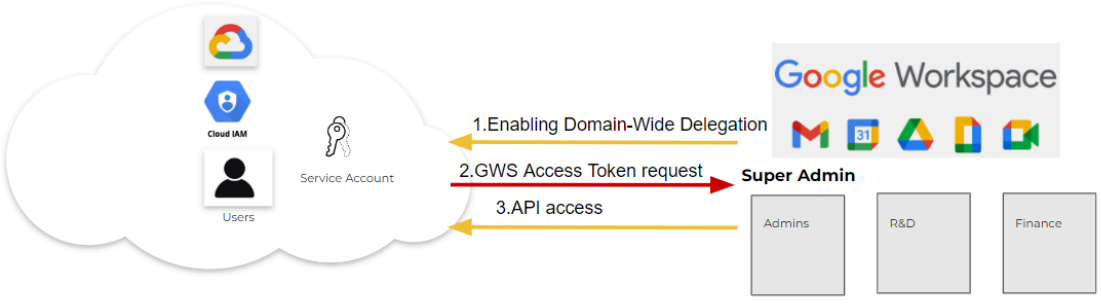

Figure 2. Domain-wide delegation flow.

When granted domain-wide delegation, a service account in Google Workspace can access user data, act on their behalf and authenticate requests to Google APIs. The specific capabilities and data accessible depend on the defined scopes.

Understanding the Risks and Implications of the Domain-Wide Delegation Feature

Once the domain-wide delegation is granted to a GCP service account, a GCP identity with the necessary permission can generate an access token to a delegated service account in the same project. A malicious insider can then use this access token to impersonate Google Workspace users, granting unauthorized access to the users' data or performing operations on their behalf.

This scenario creates a mismatch between the sensitivity of the domain-wide delegation permission and the permission model managed on the GCP platform.

Google documentation includes a cautionary notice concerning the domain-wide delegation feature, which outlines the significant capabilities of this feature. Google mentions that, “For this reason, only super admins can manage domain-wide delegation, and they must specify each API scope that the app can access.”

Google has an article suggesting not using automatic role grants for Service Accounts, which in the described case would have prevented the creation of a default Google Compute Engine Service Account. To help reduce excess permissions, Google has documentation on GCP role recommendations best practices, which also mentions their "Recommender API" tool.

Using Audit Logs From Both Ends to Identify Potential Misuse

It is impossible to understand the complete picture of the activity and identify any potential misuse of the domain-wide delegation feature without analyzing the audit logs from both platforms, GCP and Google Workspace. The generation of a service account key log will appear in GCP logs while Google key generation and API call execution logs will appear in Google Workspace logs.

In Figure 3, there is an XQL query from the Cortex web interface that is searching for service account key creation in GCP audit logs.

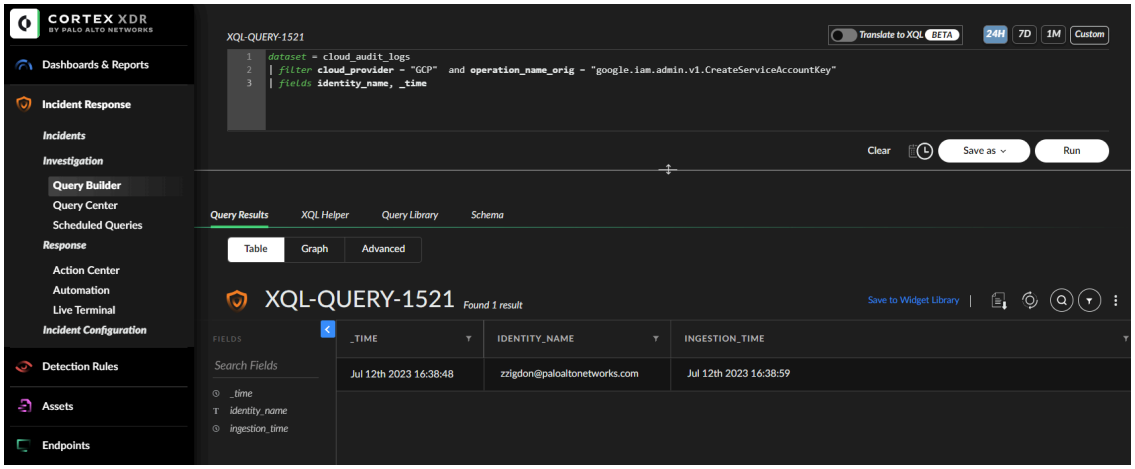

Figure 3. Searching for service account key creation.

```
event from cloud.audit_logs where cloud.type = 'gcp' AND operation = 'google.iam.admin.v1.CreateServiceAccountKey' ADDCOLUMN $.payload.resourceName $.timestamp
```

Figure 4. Equivalent query in Prisma Cloud RQL syntax.

Figure 5 shows an XQL query that searches for the service account authorization log.

```
XQL-QUERY-1522
1  dataset = saas_audit_logs
2  | filter service_type = "TOKEN" and operation_name_orig = "authorize"
3  | fields identity_name
```

Figure 5. Searching for the Google Workspace access token request.

```
event from cloud.audit_logs where cloud.type = 'gcp' AND json.rule = $.payload.resourceName = 'TOKEN' AND $.payload.authorizationInfo[0].granted = 'true'
ADDCOLUMN $.payload.resourceName
```

Figure 6. Equivalent query in Prisma Cloud RQL syntax.

Figure 7 shows we checked who gave this service account domain-wide delegation permission and when that happened.

```
XQL-QUERY-1522
1  dataset = saas_audit_logs
2  | filter operation_name_orig = "AUTHORIZE_API_CLIENT_ACCESS"
3  | fields identity_name
```

Figure 7. Searching for the log that indicates that domain-wide delegation permissions were granted to a service account.

```
event from cloud.audit_logs where cloud.type = 'gcp' AND json.rule = $.payload.resourceName = 'TOKEN' ADDCOLUMN $.payload.resourceName
$.payload.authenticationInfo.principalSubject
```

Figure 8. Equivalent query in Prisma Cloud RQL syntax.

Figure 9 shows the alert “A Google Workspace admin has enabled domain-wide delegation to a GCP service account and granted him access to a sensitive scope” was triggered in the Cortex web interface.

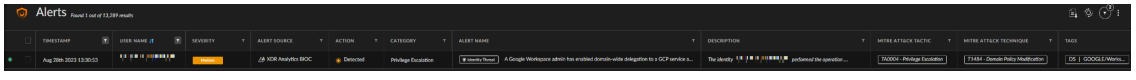

Figure 9. Domain-wide delegation alert in the Cortex web interface.

Mitigation

The security risk we have identified lies in the mismatch between the initial permissions necessary for a malicious insider to misuse the domain-wide delegation feature and the potential impact.

Optimal security practices for service accounts with domain delegation permissions are to position them within a higher-level folder in the GCP hierarchy. In the GCP hierarchy model, access control is hierarchical.

Permissions and policies set at a higher level (e.g., organization or folder) do not automatically grant access to lower-level folders or projects. Access control is not inherited downward in the hierarchy, meaning that lower-level folders or projects do not have automatic access to higher-level ones.

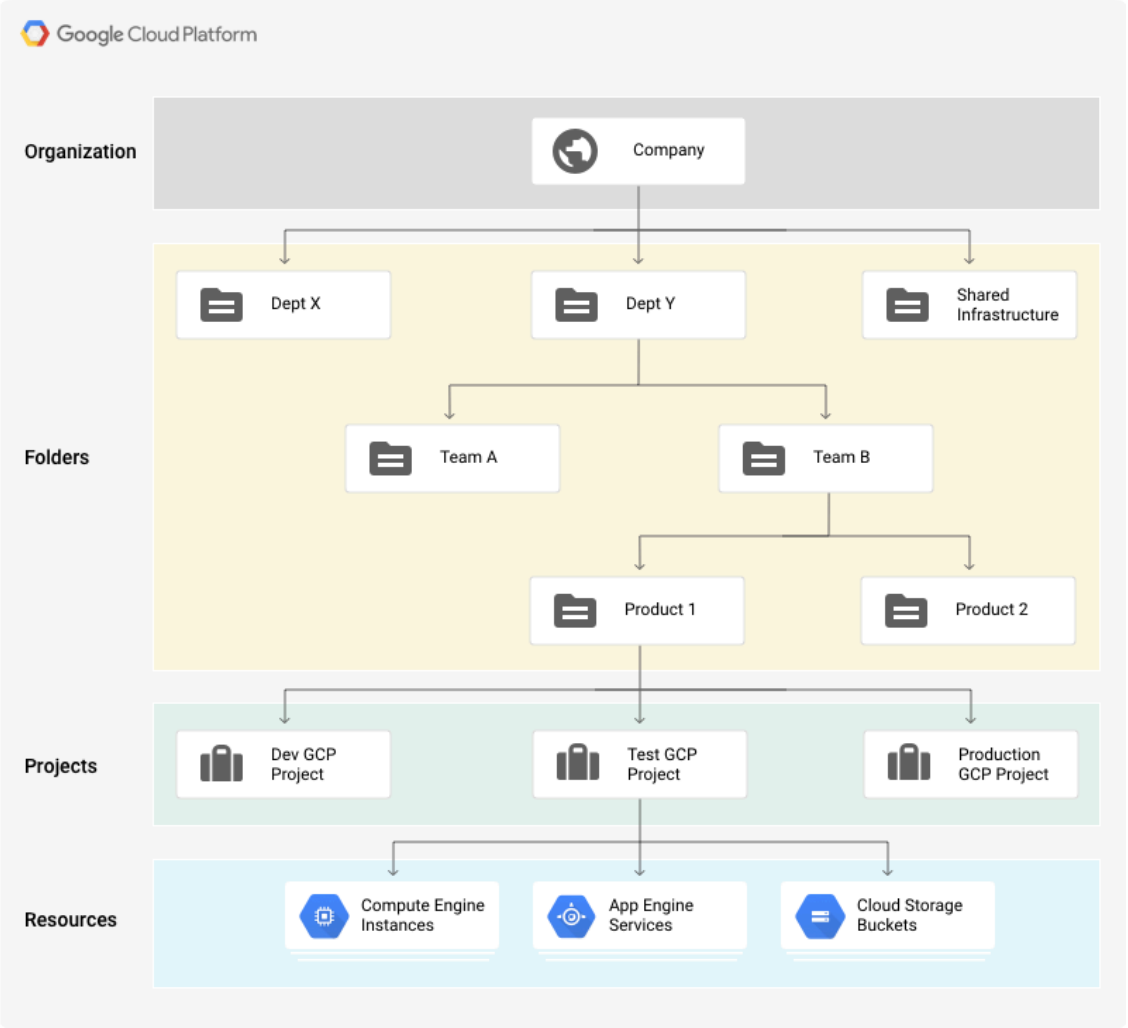

Figure 10. GCP resource hierarchy tree

This strategy reduces the surface area for security breaches by potential malicious insiders who would normally only have permissions within lower-level folders or projects within the GCP hierarchy shown in Figure 10. You can stop entities in lower-level areas from getting the service account's access tokens by making sure that only entities in the same or higher-level folders or projects can generate access tokens to the delegated service account. This helps prevent the misuse of domain-wide delegation permissions and prevents access to Google Workspace data.

Conclusion

We've been discussing this issue with Google through a variety of contact points since June 2023. This issue was also identified by Team Axon, which they have also reported to Google.

There are risks and implications associated with the domain-wide delegation feature that security defenders need to consider when configuring this permission. Depending on the scope that was granted with the domain-wide delegation, an attacker can use the feature to impersonate Google Workspace users, perform actions on their behalf and gain unauthorized access to their data.

It's important to highlight the mismatch between the initial permissions required for the attacker to misuse this feature, and the possible impact. In worst cases, an attacker or a malicious insider can leak sensitive Google Workspace data, such as emails, documents, and other confidential information stored within the domain.

Palo Alto Networks customers receive protection from the issue discussed in this article through both Cortex XDR and Prisma Cloud.

Cortex XDR capabilities can identify and alert on various abnormal activities such as the granting of domain wide delegation permissions or the creation of GCP service account keys. Cortex XDR is able to learn the behavior of GCP and Google Workspace entities and detect unusual behavior.

Prisma Cloud CIEM can help mitigate risky and over-privileged access by providing:

- Visibility, alerting, and automated remediation on risky permissions
- Automatic findings of unused permissions with Least-privilege access remediations

Prisma Cloud Threat Detection capabilities can alert on various identity-related anomalous activities such as unusual usage of credentials from inside or outside of the cloud.

Prisma Cloud can also perform runtime operation monitoring and provide governance, risk and compliance (GRC) requirements for any component associated with their cloud environment.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Disclosure Timeline

- **June 27, 2023:** Palo Alto Networks submitted a report about the domain-wide delegation security risk to the Google Workspace product team.
- **July 10, 2023:** Security discussion between Google Workspace product team and Palo Alto Networks cloud research group.

- **July 18, 2023:** Palo Alto Networks submitted a report to the Google Vulnerability Reward Program regarding this issue.
- **Aug. 2, 2023:** Palo Alto Networks filed a bug with the Google Workspace product team and they replied that they would implement a fix if required.
- **August 2023:** Palo Alto Networks notified Google of the intention to publish on the security risk and offered the opportunity for fixes or input.
- **Nov. 8, 2023:** Palo Alto Networks invited Google's input on our article on the domain-wide delegation security risk.
