WEBINAR SUMMARY

September 3, 2020

GCP Lateral Movement and Privilege Escalation: Spillover and Updates from Google

Dylan Ayrey, Security Engineer
Michael Sanders, Senior Cloud Security Engineer, ExtraHop

KEY TAKEAWAYS

- Original talk summary: GCP roles are often cross-project, which created security holes.
- Google has made some security updates, including to GCP roles.
- Privilege escalation remains an issue across the GCP.
- The shift to detection and response is helping security operations regain control of the cloud.
- ExtraHop offers visibility into GCP workloads, speeding up detection and response.

in partnership with

OVERVIEW

Lateral movement and privilege escalation present significant security challenges to users of Google Cloud Platform (GCP). Since Dylan Ayrey's Blackhat 2020 talk on the subject, Google has announced changes that will improve security in some areas, while other problematic areas remain.

Because potential security holes can't always be prevented—there are too many potential paths in and some are deemed "working as designed"—Security Operations (Sec Ops) teams need to focus instead on detection and response. Network detection and response (NDR) solutions like ExtraHop's Reveal(x) 360 can help Sec Ops teams quickly identify security problems and respond efficiently and effectively.

CONTEXT

Dylan Ayrey provided an update on the GCP lateral movement and privilege escalation talk he co-presented at Blackhat 2020 and shared additional information on security issues he was not able to cover during that presentation. Michael Sanders discussed the importance of detection and response for Sec Ops professionals working in cloud environments.

KEY TAKEAWAYS

Original talk summary: GCP roles are often cross-project, which created security holes.

Dylan Ayrey summed up the key takeaways from his talk at Blackhat 2020 about GCP lateral movement and privilege escalation. This talk focused on security challenges created by cross-project GCP roles.

Key Takeaways: Dangers of Cross-Project Roles in GCP

- **Roles are often cross-project,** and the cross-project bindings are difficult to see because of the resource-centric nature of policies in GCP. There is no way to know what access service accounts have.
- **Top-suggested roles are dangerous.** Unless service accounts are explicitly assigned, roles are automatically given an overly permissive service account that has the project editor role, with thousands of permissions granted by default and new permissions added each time Google creates new services.
- **Some roles can elevate themselves to the project editor role** when the default editor identity is attached, which provides access to cross-project service accounts.

> It is a common pattern for people to think projects provides this nice, secure, isolated boundary between other projects. What we found through investigation was this wasn't really the case.
>
> *Dylan Ayrey*

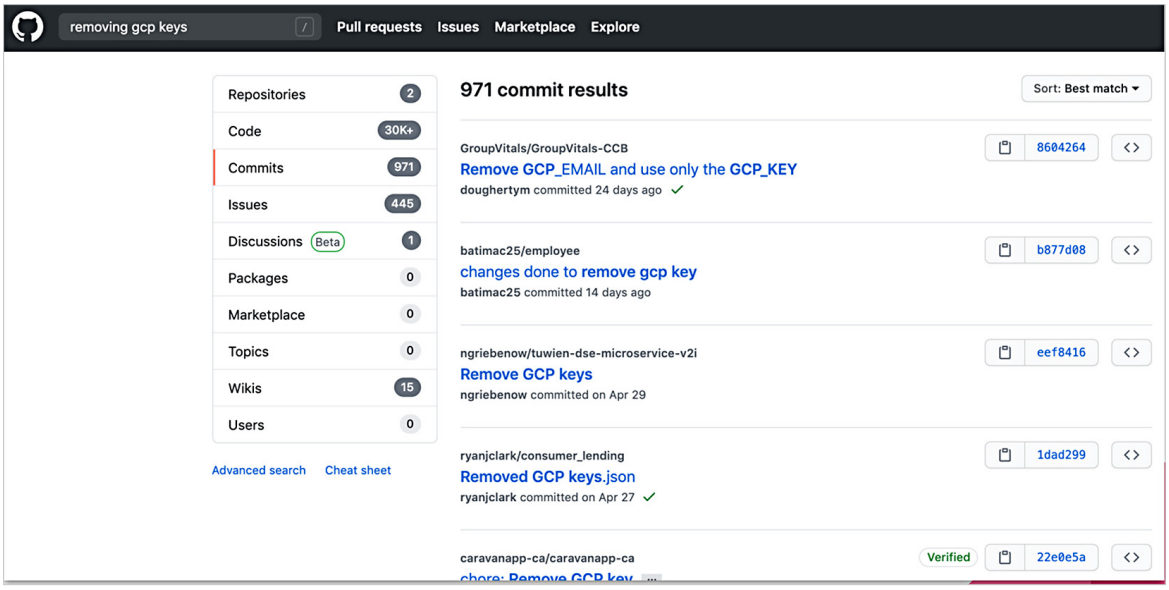
Google has made some security updates, including to GCP roles.

Since the original talk, Google has made updates to improve security. One significant change is coming to roles in 2021, requiring actAs permissions for roles to act as service account. This will ensure that users with access to the Compute Engine default service account do not have unintended Identity and Access Management (IAM) permissions.

While this change prevents access to the default service account, which improves security, the downside is that developers are likely to make actAs changes at the project level, and not the role level. Security professionals will need to closely monitor the use of dangerous permissions found at the project level—and specifically these actAs permissions—to ensure the right access is granted to the right service accounts and right projects.

Additionally, Google has now made it more challenging to gain an initial foothold into a system by pulling keys that could have provided privilege escalation and lateral movement into highly permissioned accounts off GitHub. The search parameters that could previously be used to identify access points have been scrubbed, although it is still possible to find access points by creatively changing queries, such as by searching on "Removing GCP Key."

Figure 1: Despite changes, initial foothold access points are still accessible with creative GitHub searches



While these changes improve security, the challenges the changes present show that security must be focused on in depth, and not just entirely on perimeter breaches.

Privilege escalation remains an issue across the GCP.

Privilege escalation (privesc) is an issue in both the Google Compute Engine and Google managed service accounts. Metadata roles and login roles both offer potential access points to the Compute Engine via privilege escalation.

Privesc concerns in Compute Engine roles	
Metadata roles	Service accounts can be compromised on instances via a startup script; permissions allow bad actors to override the startup scripts with their own code: – compute.instances.setMetadata (to affect a single instance) – compute.projects.setCommonInstanceMetadata (to affect all instances in the project)
Login roles	Login roles typically granted to developers to debug instances allow service account compromise via secure shell (SSH). Bad actors can take control of service accounts with overly permissive roles, or even take over roles in other projects. – roles/compute.osLogin – roles/compute.osAdminLogin

Privilege escalation can also occur through Google managed service accounts that Google, not the organization, controls. These accounts are used to power application programming interfaces (APIs), such as cloud build, remote build execution (RBE), deployment manager, and others. They typically give access to data and sometimes IAM; they can be used by bad actors to steal short-lived credentials that can be used to access higher privilege, more permanent access to the project.

The shift to detection and response is helping security operations regain control of the cloud.

These sheer number of roles and permissions, and other potential access points into cloud platforms like GCP, are causing Sec Ops to lose control and visibility in the cloud. The shift from protection and prevention alone to network detection and response is helping Sec Ops regain that visibility and control.

Figure 2: Sec Ops are losing control and visibility on the cloud

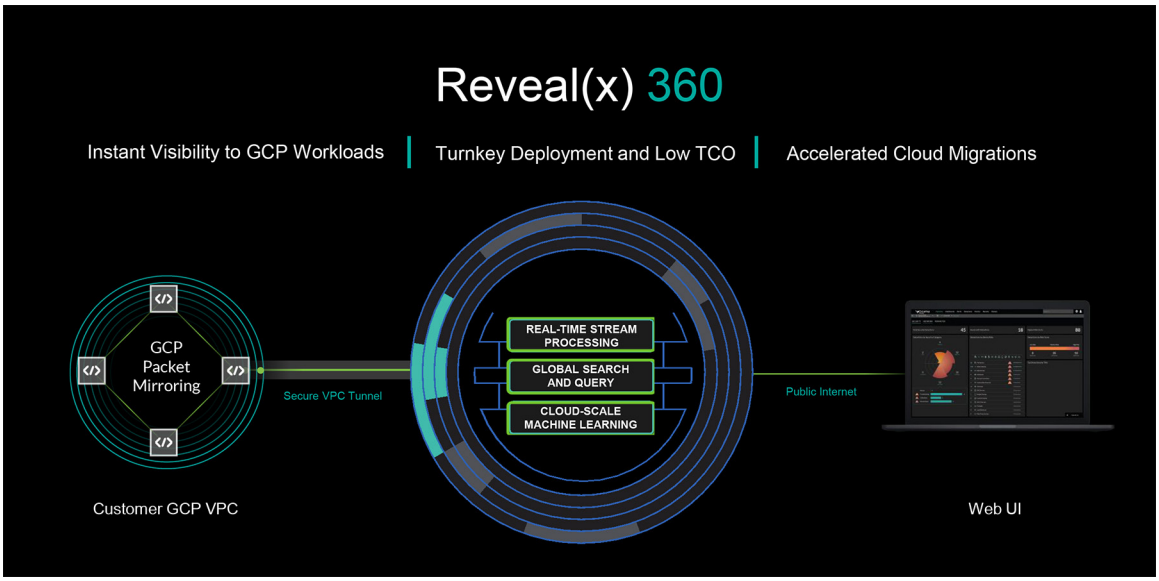
NDR looks at the truth of the network, assuming that with all of the services, roles, and access points in the cloud, including ones the organization has minimal or no control over, breaches are going to happen. Sec Ops uses these solutions to identify problems and respond to them quickly and efficiently.

> We have to assume that some kind of compromise is happening. We want to be able to detect and respond before we get to the the real damage that's going to happen.
>
> *Michael Sanders*

ExtraHop offers visibility into GCP workloads, speeding up detection and response.

ExtraHop Reveal(x) 360 offer instant visibility into GCP workloads, enabling Sec Ops professionals to detect and respond to security issues at the speed of the cloud. ExtraHop's solution offers application layer decoding, line rate decryption, detection and investigation tools that ensure problems are noticed, and automated response.

Figure 3: Reveal(x) 360 offers instant visibility into GCP workloads.



ADDITIONAL INFORMATION

- **For more information on privilege escalation in GCP:** Read Chris Moberly's Tutorial on privilege escalation and post-exploitation tactics in Google Cloud Platform environments at GitLab.
- **Follow Dylan Ayrey** on Twitter: @InsecureNature.
- **Work with Google:** With over 3,150 permissions and more than 54 APIs, organizations are likely to run into other security concerns. To address these concerns:
  - Use Google's Vulnerability Reward Program (known as Google Bug Bounty) to report issues.
  - Reach out to Google support if reported bugs are returned as working as designed. It is important to be persistent as Google will usually work with organizations to help resolve issues.

BIOGRAPHIES

Dylan Ayrey

Security Engineer

Dylan Ayrey is a Security Engineer. He has been heavily involved in the open source community for a few years, and he has been doing his best to bring security practices into the cloud/devsecops world.

Michael Sanders

Senior Cloud Security Engineer, ExtraHop

Michael is responsible for architecting security implementations across hyper-converged networks and is part of ExtraHop's team of cloud security engineers who work directly with customers and prospects. A passionate technologist and evangelist, he brings fresh thinking to security threat detection. Prior to ExtraHop, Michael was a consultant working with multiple technologies across the securitylandscape. He holds a Masters Degree from the University of Arizona and a BBA from the University of Georgia. Michael speaks at industry events, supports security research organizations, and has been quoted in industry coverage.

© 2020 Informa. All rights reserved.