RCE in Google Cloud Deployment Manager: A $133,337 DevSecOps lesson

Overview and reflections by Ayub Atif

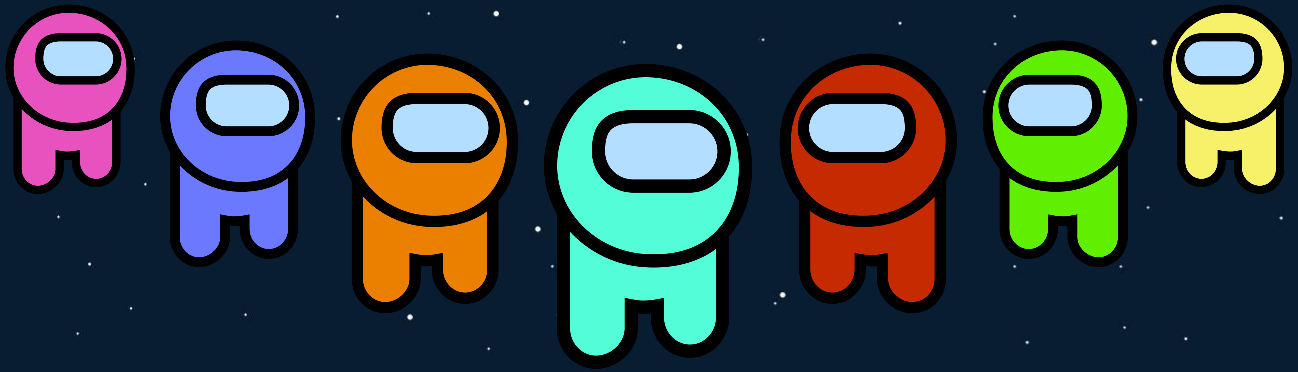


Table of Contents

01

Motivation

What's Google Cloud Deployment Manager?

02

Technical

What were the vulnerabilities and how were they found?

03

Reflection

How does this influence how we think of such devops platforms?

04

Takeaways

How can one get into bug bounties?
Hacking mindset?

The Google Cloud Deployment Manager (GCDM)

Declarative parallel repeatable templates with a console UI

REST API based (v2)

A descriptor document describes an API and it's resources (v2beta)

How can we attack this?

Photo by Google Cloud

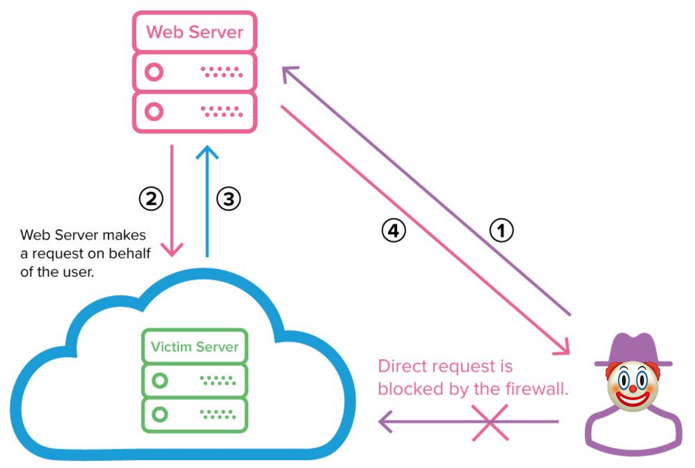
Provides info on resources

Security 101: Server-Side Request Forgery (SSRF)

Abuse target URLs to read data from services not exposed to internet

Modify target URLs for vulnerable app

Expose an internal endpoint

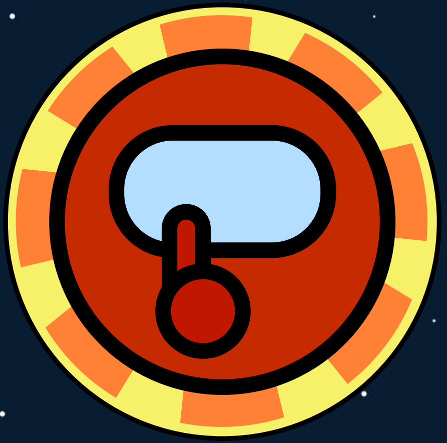

Web Server
②
③
Web Server makes a request on behalf of the user.
④
①
Victim Server
Direct request is blocked by the firewall.

AWS metadata, no auth NoSQL, internal tools

Bypass direct request firewall

Whoa!

This presentation involves following a whitehat's hacking adventure. To guarantee an organized ordeal, questions and audience interaction are delayed for the end of the presentation!



GCDM Attack angles

API-based interaction

Hidden resource Types?

Type provider system

Endpoint pointing to internal Google APIs?

Template based deployments

Malicious python templates?

Something else?

Is there any unintended behavior to exploit?

Hidden resource Types?

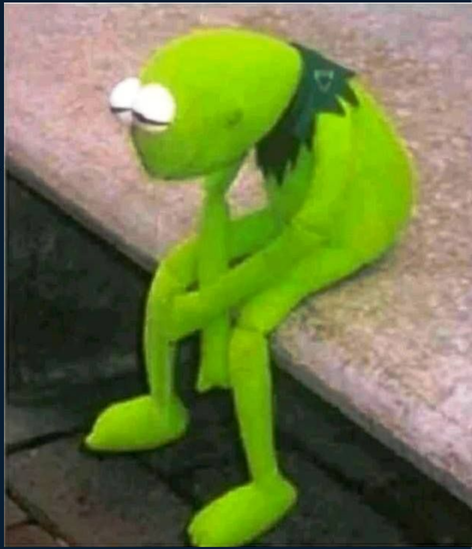
None found...

Malicious Template?

Templates interpreted on isolated container...

Type provider?

Internal endpoint leads to invalid descriptor document...



"Beware of old package versions in your project with security vulnerabilities"

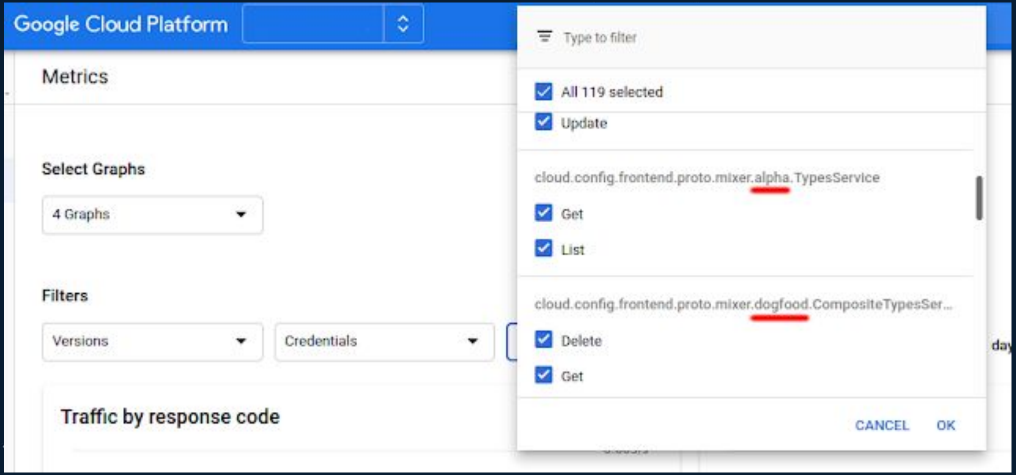
BUMPED BY SMART PACKAGE MANAGERS

"What about other versions of GCDM methods?"

Unintended public API versions

Methods often include API version in names

Alpha wasn't very interesting, but dogfood...



Google Cloud Platform

Metrics

Select Graphs

4 Graphs

Filters

Versions

Credentials

Traffic by response code

Type to filter

☑ All 119 selected

☑ Update

cloud.config.frontend.proto.mixer.alpha.TypesService

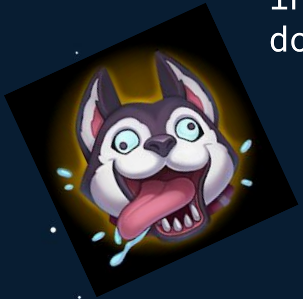
☑ Get

☑ List

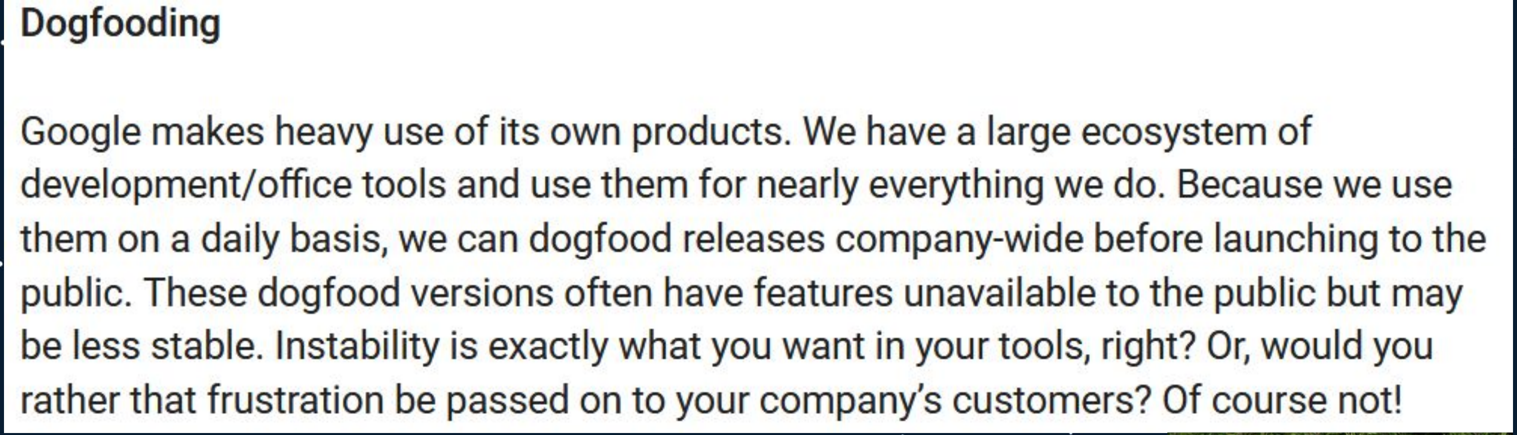
cloud.config.frontend.proto.mixer.dogfood.CompositeTypesSer...

☑ Delete

☑ Get



Google Testing Blog: Dogfood



Dogfooding

Google makes heavy use of its own products. We have a large ecosystem of development/office tools and use them for nearly everything we do. Because we use them on a daily basis, we can dogfood releases company-wide before launching to the public. These dogfood versions often have features unavailable to the public but may be less stable. Instability is exactly what you want in your tools, right? Or, would you rather that frustration be passed on to your company's customers? Of course not!

Anthony Vallone

Staff Software Engineer @ Google

Exploring Dogfood

googleOptions is unique to dogfood version of methods

No clue on valid credentialType or transport...

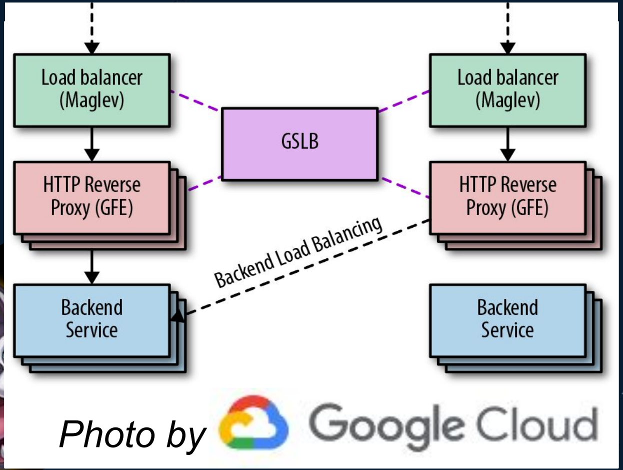
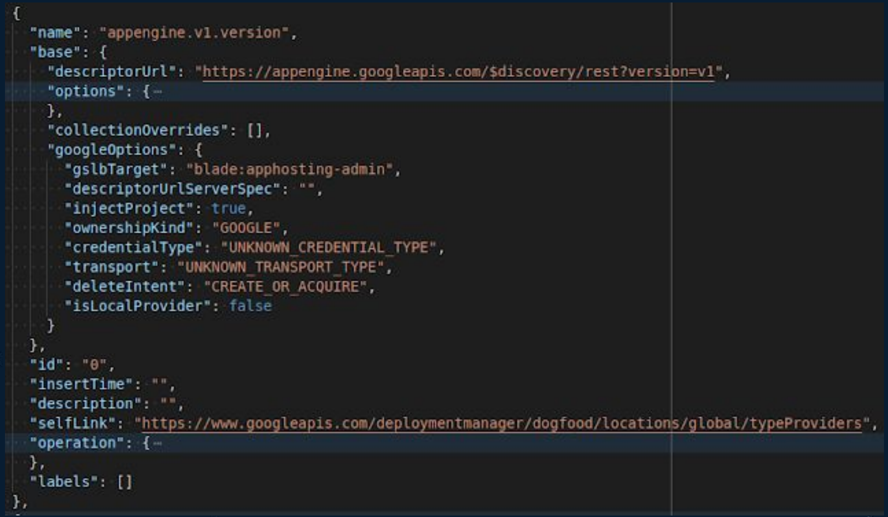


Photo by Google Cloud



```
{
  "name": "appengine.v1.version",
  "base": {
    "descriptorUrl": "https://appengine.googleapis.com/$discovery/rest?version=v1",
    "options": {⋯
    },
    "collectionOverrides": [],
    "googleOptions": {
      "gslbTarget": "blade:apphosting-admin",
      "descriptorUrlServerSpec": "",
      "injectProject": true,
      "ownershipKind": "GOOGLE",
      "credentialType": "UNKNOWN_CREDENTIAL_TYPE",
      "transport": "UNKNOWN_TRANSPORT_TYPE",
      "deleteIntent": "CREATE_OR_ACQUIRE",
      "isLocalProvider": false
    }
  },
  "id": "0",
  "insertTime": "",
  "description": "",
  "selfLink": "https://www.googleapis.com/deploymentmanager/dogfood/locations/global/typeProviders",
  "operation": {⋯
  },
  "labels": []
},
```

Protocol Buffers

Google

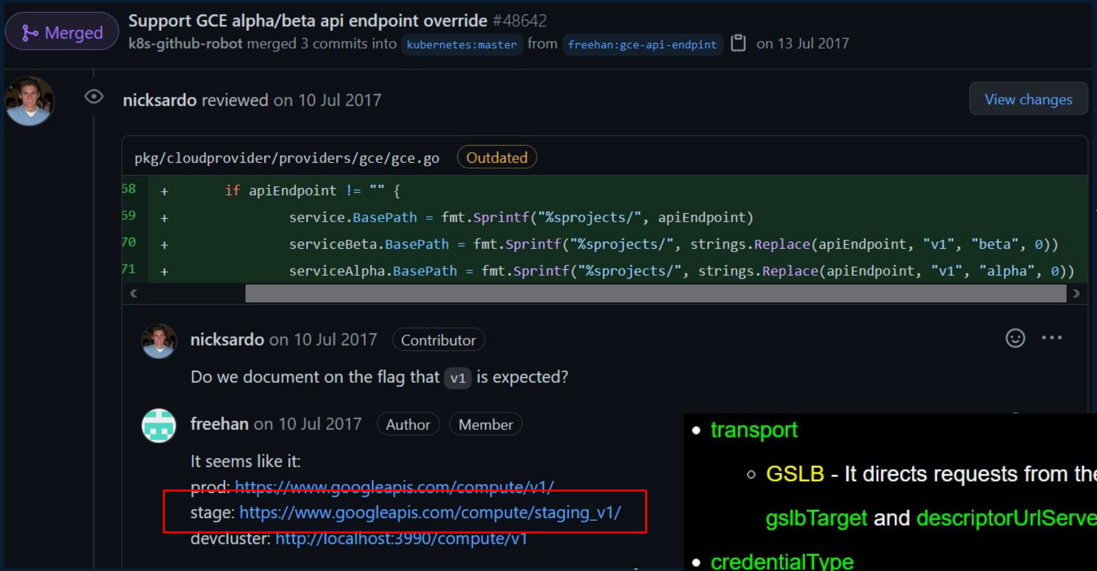
- Develops protobuf for serializing structured data
- Protobuf used in their REST competitor gRPC
- Experimental gRPC Fallback ‘Proto over HTTP’ is on most Google APIs

Our Hacking Protagonist

- Enums in protobuf are represented as integers not Strings
- Proto over HTTP is supported on GCDM API
- Comparing JSON and protobuf responses on calling get Type Provider of API, then reverse engineer required values

Google Compute Engine fake API Success

Proto over HTTP on Staging environment



Support GCE alpha/beta api endpoint override #48642

k8s-github-robot merged 3 commits into `kubernetes:master` from `freehan:gce-api-endpint` on 13 Jul 2017

nicksardo reviewed on 10 Jul 2017

pkg/cloudprovider/providers/gce/gce.go Outdated

```
+       if apiEndpoint != "" {
+               service.BasePath = fmt.Sprintf("%sprojects/", apiEndpoint)
+               serviceBeta.BasePath = fmt.Sprintf("%sprojects/", strings.Replace(apiEndpoint, "v1", "beta", 0))
+               serviceAlpha.BasePath = fmt.Sprintf("%sprojects/", strings.Replace(apiEndpoint, "v1", "alpha", 0))
```

nicksardo on 10 Jul 2017 Contributor

Do we document on the flag that `v1` is expected?

freehan on 10 Jul 2017 Author Member

It seems like it:
prod: https://www.googleapis.com/compute/v1/
stage: https://www.googleapis.com/compute/staging_v1/
devcluster: http://localhost:3990/compute/v1

Note that service account credentials tokens used by GCDM are delegated to the user-profile level instead

- transport
  - GSLB - It directs requests from the *Deployment Manager* to the internal Google endpoints specified in gslbTarget and descriptorUrlServerSpec
- credentialType
  - ENDUSERCREDS, TYPE_CREDENTIAL - They seem to act the same way as OAUTH and UNKNOWN_CREDENTIAL_TYPE

“Check the access control AS WELL AS the information flow control of your CI/CD environment”

The Second part can provide valuable clues to attackers

Relating the vulnerabilities to other DevOps platforms you may work on

Google Cloud

Microsoft Azure

aws

GitHub

DEVSECOPS CHALLENGES

Integration reluctance

Cross-platform team
knowledge sharing culture

↔

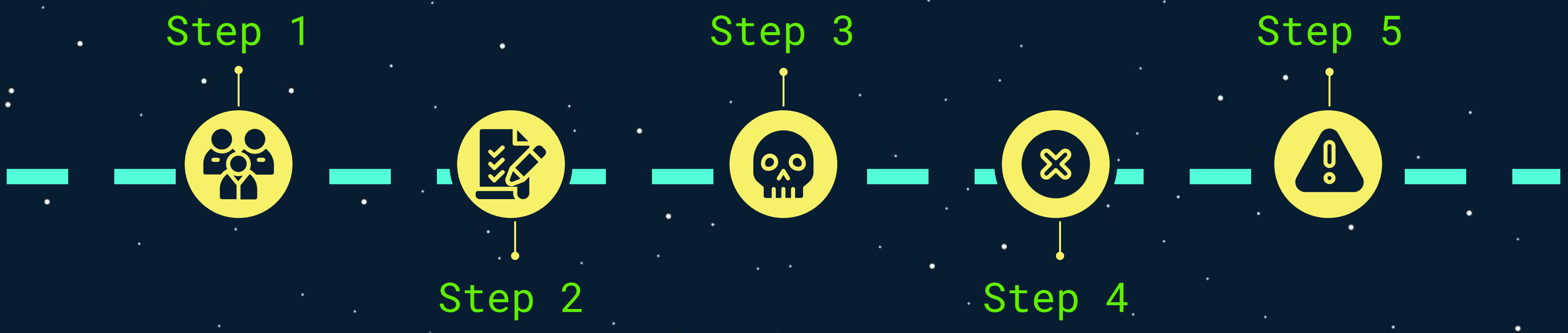
Developer security knowledge

Devsecops developers should have a
basic level of security skills

Friction-less pipeline

Inclusion of security
should be effortless, not
overloading developers

Bug Bounty?



Step 1

Whitehat explores vulnerabilities

Step 2

Report of exploit(s) sent to company

Step 3

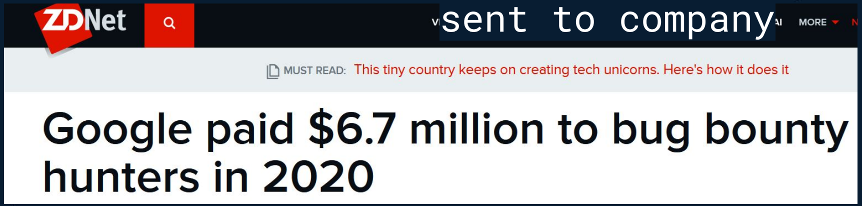
Whitehat respects the limits as per computer fraud and abuse act

Step 4

Company reviews report and assigns issue to engineers

Step 5

Whitehat is (often) compensated for the discovery



MUST READ: This tiny country keeps on creating tech unicorns. Here's how it does it

Google paid $6.7 million to bug bounty hunters in 2020

"Enjoy the challenges and learning process, focus not solely on the end but on the journey as well"

THE ZEN OF HACKING

Average script kiddie

Average hacking enjoyer

RCE Vulnerability discovered and documented by Ezequiel Pereira

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik**

https://defendtheweb.net/?hackthis **https://www.hackthebox.eu/**

https://hackerone.com/bug-bounty-programs