YES WE HACK

#YWH-PGM4091-29 ASK FOR FIX VERIFICATION REWARD : $100.00

/ Google Maps API key on analytics.pinelabs.com

PINE LABS BUG BOUNTY PROGRAM

SUBMITTED BY ADITYASHENDE ON 2023-01-27

REPORT DETAILS

BUG TYPE	Improper Access Control - Generic (CWE-284)
SCOPE	analytics.pinelabs.com
ENDPOINT	https://analytics.pinelabs.com/public/resources/theme/default/js/utility.js/hopfully404
SEVERITY	High
VULNERABLE PART	others
PART NAME	AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons
PAYLOAD	https://analytics.pinelabs.com/public/resources/theme/default/js/utility.js/hopfully404
TECHNICAL ENVIRONMENT	Windows 10 , Chrome
APPLICATION FINGERPRINT	
IP USED	103.163.91.24

CVSS SCORE	SEVERITY
8.6	HIGH

VECTOR STRING

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

BUG DESCRIPTION

Description

Google Maps API is a paid service which allows applications to embed & search from the Google Maps Database and use it on their own applications. While some of the services was free at the back times of Early 2018, they changed their usage plan after that date. Since then, developers need to use an API key or client-id solution for all of the API's they are using from.

These API keys have some security configurations for blocking unauthorized usage for malicious people which does not comes by default.

Exploitation

OPEN the URLs

1. API key is vulnerable for Places Photo API! Here is the PoC link which can be used directly via browser:

https://maps.googleapis.com/maps/api/place/photo?maxwidth=400&photoreference=CnRtAAAATLZNl354RwP_9UKbQ_5Psy40texXePv4oAlgP4qNEkdIrkyse7rPXYGd9D_Uj1rVsQdWT4oRz4QrYAJNpFX7rzqqMlZw2h2E2y5IKMUZ7ouD_SlcHxYq1yL4KbKUv3qtWgTK0A6QbGh87GB3sscrHRIQiG2RrmU_jF4tENr9wGS_YxoUSSDrYjWmrNfeEHSGSc3FyhNLIBU&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

1. API key is vulnerable for Place Details API! Here is the PoC link which can be used directly via browser:

https://maps.googleapis.com/maps/api/place/details/json?place_id=ChIJN1t_tDeuEmsRUsoyG83frY4&fields=name,rating,formatted_phone_number&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

1. API key is vulnerable for Nearby Search-Places API! Here is the PoC link which can be used directly via browser:

https://maps.googleapis.com/maps/api/place/nearbysearch/json?location=-33.8670522,151.1957362&radius=100&types=food&name=harbour&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

1. API key is vulnerable for Text Search-Places API! Here is the PoC link which can be used directly via browser:

https://maps.googleapis.com/maps/api/place/textsearch/json?query=restaurants+in+Sydney&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

1. API key is vulnerable for Directions API! Here is the PoC link which can be used directly via browser:

https://maps.googleapis.com/maps/api/directions/json?

origin=Disneyland&destination=Universal+Studios+Hollywood4&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

1. API key is vulnerable for Geocode API! Here is the PoC link which can be used directly via browser:

https://maps.googleapis.com/maps/api/geocode/json?latlng=40,30&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

1. API key is vulnerable for Distance Matrix API! Here is the PoC link which can be used directly via browser:

https://maps.googleapis.com/maps/api/distancematrix/json?units=imperial&origins=40.6655101,-73.89188969999998&destinations=40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.659569%2C-73.933783%7C40.729029%2C-73.851524%7C40.6860072%2C-73.6334271%7C40.598566%2C-73.7527626%7C40.659569%2C-73.933783%7C40.729029%2C-73.851524%7C40.6860072%2C-73.6334271%7C40.598566%2C-73.7527626&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

1. API key is vulnerable for Find Place From Text API! Here is the PoC link which can be used directly via browser:

https://maps.googleapis.com/maps/api/place/findplacefromtext/json?input=Museum%20of%20Contemporary%20Art%20Australia&inputtype=textquery&fields=photos,formatted_address,name,rating,opening_hours,geometry&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

1. API key is vulnerable for Autocomplete API! Here is the PoC link which can be used directly via browser:

https://maps.googleapis.com/maps/api/place/autocomplete/json?input=Bingh&types=%28cities%29&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

Risk

HTTP Referrers: Restricts apps via HTTP Referrer headers which are defined to. Wildcards can be used for multiple domains/paths such as *example.com/*. However be careful when using, because some bypass techniques can be used if the wildcard is defined such as *example.com or example.com*, within the payloads of ozguralpexample.com and example.com.ozguralp.com domains in order.

IP Addresses: If the key will be used for just one application such as server-to-side solutions, this configuration could have been best fit for you.

Android/iOS Apps: If you are going to use the key via mobile apps, this restrictions will also work for you.

/ Impact:

If the API keys are not met with these security configurations, below scenarios may be conducted by a malicious user:

Consuming the company’s monthly quota or can over-bill with unauthorized usage of this service and do financial damage to the company, if the company does not have any limitation settings on API budgets.
Conduct a denial of service attack specific to the service if any limitation of maximum bill control settings exist in the Google account. While this could not be too dangerous if used the application parts of such “Contact Us” pages, however it could be really dangerous if the main business/functionality of the app is handled within these maps such as Uber (Finding/tracking rides via Maps) and Booking (Searching hotels via Maps).

Remediation

IP, Referrer or App restriction check controls should be applied.

It can be considered using the client id authentication solution and signatures rather than API keys.

For best practices, not used APIs show be disabled for lowering the exploitable level.

COMMENTS

ADITYASHENDE ON 2023-01-27 10:22:41

NEW

PINE LABS PVT LTD ON 2023-01-27 10:24:31

NEW → UNDER REVIEW

Hi ADITYASHENDE,

Thanks for your submission.

Your report will be reviewed by our team and updated in a timely manner.

Regards.

PINE LABS PVT LTD ON 2023-01-27 10:32:28

Updated report details.

Bug type	Use of Hard-coded Cryptographic Key (CWE-321) → Use of Hard-coded Cryptograph
Endpoint	view-source:https://analytics.pinelabs.com/public/resources/theme/default/js/utility.
Part name	Search for AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons → AIzaSyAMpkFI4TQDZ
Payload	Multiple → https://analytics.pinelabs.com/public/resources/theme/default/js/utility.js

PINE LABS PVT LTD ON 2023-01-27 10:32:52

Updated report title.

API KEY exploitable for multiple methods can lead to financial loss of services → Google Maps API key on analytics.pinelabs.com

PINE LABS PVT LTD ON 2023-01-30 10:37:41

UNDER REVIEW → ACCEPTED

Hello,
We were able to reproduce the PoC and we decided to accept your report.
Your report is therefore eligible for a reward – stay tuned.
Congrats/Cheers,

ADITYASHENDE ON 2023-01-31 08:05:56

Thanks

PINE LABS PVT LTD ON 2023-02-15 07:45:51

$100.00 and **11 pts** rewarded to **ADITYASHENDE**

ADITYASHENDE ON 2023-02-18 11:20:03

Why the bounty range is low ? The report marked as High !!!

PINE LABS PVT LTD ON 2023-02-20 09:20:18

3 pts awarded for report quality.

PINE LABS PVT LTD ON 2023-03-02 08:24:54

ACCEPTED → ASK FOR FIX VERIFICATION

Hello,
A fix has been deployed for this vulnerability.
Could you please verify that you cannot reproduce the bug nor bypass the fix ?
Thanks for your help,
Regards,

ADITYASHENDE ON 2023-03-12 05:35:33

I am still able to recreate bug the bug.

PINE LABS PVT LTD ON 2023-03-14 06:40:14

Hi Researcher,

Thank you for the revalidation, it would be great if you can attach latest evidences for the same.

Thank you.

ADITYASHENDE ON 2023-03-14 09:08:39

API key is vulnerable for Directions API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/directions/json?
origin=Disneyland&destination=Universal+Studios+Hollywood4&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Geocode API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/geocode/json?
latlng=40,30&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Distance Matrix API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/distancematrix/json?units=imperial&origins=40.6655101,-73.89188969999998&destinations=40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.659569%2C-73.933783%7C40.729029%2C-73.851524%7C40.6860072%2C-73.6334271%7C40.598566%2C-73.7527626%7C40.659569%2C-73.933783%7C40.729029%2C-73.851524%7C40.6860072%2C-73.6334271%7C40.598566%2C-73.7527626&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Find Place From Text API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/findplacefromtext/json?
input=Museum%20of%20Contemporary%20Art%20Australia&inputtype=textquery&fields=photos,formatted_address,name,rating,opening_hours,geometry&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Autocomplete API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/autocomplete/json?
input=Bingh&types=%28cities%29&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Elevation API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/elevation/json?locations=39.7391536,-104.9847034&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Place Details API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/details/json?
place_id=ChIJN1t_tDeuEmsRUsoyG83frY4&fields=name,rating,formatted_phone_number&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Nearby Search-Places API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/nearbysearch/json?location=-33.8670522,151.1957362&radius=100&types=food&name=harbour&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Text Search-Places API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/textsearch/json?
query=restaurants+in+Sydney&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Places Photo API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/photo?
maxwidth=400&photoreference=CnRtAAAATLZNl354RwP_9UKbQ_5Psy40texXePv4oAlgP4qNEkdIrkyse7rPXYGd9D_Uj1rVsQdWT4oRz4QrYAJNpFX7rzqqMlZw2h2E2y5IKMUZ7ouD_SlcHxYq1yL4KbKUv3qtWgTK0A6QbGh87GB3sscrHRIQiG2RrmU_jF4tENr9wGS_YxoUSSDrYjWmrNfeEHSGSc3FyhNLlBU&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Query Autocomplete-Places API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/queryautocomplete/json?
input=pizza+near%20par&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

ADITYASHENDE ON 2023-07-28 11:41:14

Any updates ?

ADITYASHENDE ON 2023-07-30 09:35:27

FIX REFUSED

Still vulnerable

API key is vulnerable for Geocode API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/geocode/json?latlng=40,30&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Distance Matrix API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/distancematrix/json?units=imperial&origins=40.6655101,-73.89188969999998&destinations=40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.6905615%2C-73.9976592%7C40.659569%2C-73.933783%7C40.729029%2C-73.851524%7C40.6860072%2C-73.6334271%7C40.598566%2C-73.7527626%7C40.659569%2C-73.933783%7C40.729029%2C-73.851524%7C40.6860072%2C-73.6334271%7C40.598566%2C-73.7527626&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Find Place From Text API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/findplacefromtext/json?input=Museum%20of%20Contemporary%20Art%20Australia&inputtype=textquery&fields=photos,formatted_address,name,rating,opening_hours,geometry&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Autocomplete API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/autocomplete/json?input=Bingh&types=%28cities%29&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Elevation API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/elevation/json?locations=39.7391536,-104.9847034&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Place Details API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/details/json?place_id=ChIJN1t_tDeuEmsRUsoyG83frY4&fields=name,rating,formatted_phone_number&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Nearby Search-Places API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/nearbysearch/json?location=-33.8670522,151.1957362&radius=100&types=food&name=harbour&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is vulnerable for Text Search-Places API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/textsearch/json?query=restaurants+in+Sydney&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons

API key is not vulnerable for Places Photo API.

API key is vulnerable for Query Autocomplete-Places API. Here is the PoC Link:
https://maps.googleapis.com/maps/api/place/queryautocomplete/json?input=pizza+near%20par&key=AIzaSyAMpkFI4TQDZAdi5gE069NMPdbRdTSUons