YES WE HACK

#YWH-PGM2368-93 INFORMATIVE REWARD : €200.00

/ Open API access disclosing PII infromation

HUAWEI CLOUD BUG BOUNTY PROGRAM

SUBMITTED BY ADITYASHENDE ON 2023-04-30

REPORT DETAILS

BUG TYPE	Insecure Storage of Sensitive Information (CWE-922)
SCOPE	*.huaweicloud.com (including *.huaweicloud.com/intl/)
ENDPOINT	/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/
SEVERITY	Medium
VULNERABLE PART	get-parameter
PART NAME	/api/
PAYLOAD	/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/
TECHNICAL ENVIRONMENT	Ubuntu WSL 18.04
APPLICATION FINGERPRINT	
IP USED	152.57.242.74

CVSS SCORE	SEVERITY
5.3	MEDIUM

VECTOR STRING

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

BUG DESCRIPTION

Summary:
The API endpoints listed below contain personally identifiable information (PII) data that is being disclosed, including phone numbers, addresses, access keys, postal codes, seller IDs, and personal information such as house addresses. This constitutes a serious breach of user privacy and security.

Affected URLs:

https://mkpdata.huaweicloud.com/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/68bcb36dcc3b41ca880d92f36422fa0e/info
https://mkpdata.huaweicloud.com/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/c712ea0471d34b1eb247ad274c6e9fca/info
https://mkpdata.huaweicloud.com/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/d87f052e8a5e3e66b0d21373058c8794/info
https://mkpdata.huaweicloud.com/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/e6a5914911394141922d0452ab86fb4b/info
https://mkpdata.huaweicloud.com/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/efc3aa0c2b7da6f10e377d52b44547ba/info
https://mkpdata.huaweicloud.com/api/marketplace/user/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/customerservice/purchaser/get-activity-guest-url
https://mkpdata.huaweicloud.com/api/marketplace/user/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/customerservice/purchaser/get-activity-url
Steps to Reproduce:

Send a GET request to any of the above-listed URLs.
The response will contain PII data, including phone numbers, addresses, access keys, postal codes, seller IDs, and personal information such as house addresses.
Impact:
The disclosure of PII data can lead to serious privacy and security issues for users. This data can be used by malicious actors for identity theft, fraud, and other illegal activities. Therefore, it is important to take immediate action to address this issue and protect user privacy.

Recommendation:

The affected endpoints should be taken down immediately until the issue is resolved.
The development team should investigate the root cause of the issue and fix it as soon as possible.
A thorough security audit should be conducted to ensure that no other endpoints or systems are vulnerable to similar data disclosure issues.
The affected users should be notified about the breach and provided with instructions on how to protect themselves from potential fraud or identity theft.
A bug bounty program should be implemented to encourage responsible disclosure of any future security vulnerabilities.

COMMENTS

ADITYASHENDE ON 2023-04-30 11:25:21

NEW

□□□□□□□□ ON 2023-05-05 09:52:05

NEW → UNDER REVIEW

Hello,
Thanks for your submission
Your report will be reviewed by our team and updated in a timely manner.
Regards.

ADITYASHENDE ON 2023-05-05 11:15:11

This has been patched

□□□□□□□□ ON 2023-05-06 05:01:13

Hello,
We still can visit these URLs and we are investigating this issue.
Regards.

ADITYASHENDE ON 2023-05-15 14:00:07

I can see its showing 403 forbidden

□□□□□□□□ ON 2023-05-17 06:07:43

Hello,
The development team has solved this issue, and the security team will review the bug bounty this week.
And we'd like to ask if you send the email to PSIRT@huawei.com to report this issue?

Best Regards.

ADITYASHENDE ON 2023-05-17 06:16:40

Thanks for update. I haven’t send any email to anyone. Just report on yeswehack

ADITYASHENDE ON 2023-05-17 06:41:05

Hey team ,
I’ve try to bypass but didn’t work but I am able to see the data using different method but not sure it can be patched. Please let me know where can I share that. Or should I make chained report for this

□□□□□□□□ ON 2023-05-17 08:12:57

Hello,

You can send the report to cloudbusoc@huawei.com with this YWH issue ID(YWH-PGM2368-93).

Best Regards.

□□□□□□□□ ON 2023-05-25 08:26:55

Hello,

We (security team) are asking development to explain key-value usage in those return result to decide the Confidentiality score in CVSS.

Best regards.

ADITYASHENDE ON 2023-05-25 10:55:11

The score represents the confidentiality of data where Sellerid, License copy URL, Access_Key,Name,Number,Address,Postal Code etc . All this information is exposed publicly and it includes orgs info where it can affect on their public reputation if some bad person exposes it. At the moment data is patched but it can be accessed or bypassed using different method so CVSS is this.

□□□□□□□□ ON 2023-05-25 11:28:40

Hello,

From my perspective, this infos are used for display to users when they browse products in Huawei Cloud Market. License copy in China (may) should be public access to customer in digital business platform. In all digital selling platform in China (including taobao, meituan, etc), customer could see the seller's company licence online. Also in physical storefront, licence needs to be mounted in a prominent place (base on national laws & regulations).

It's only my personal opinion, bug bounty decision will be made base on our bug bounty rules and real impact after development team reply to us. :)

Best Regards.

ADITYASHENDE ON 2023-05-25 12:13:38

What about other data like number , address , postal and access key

ADITYASHENDE ON **2023-05-25 12:16:32**

I’ve question that you said bug bounty will be discussed in this week. So is it confirmed that I’ll get a bounty ? :)

□□□□□□□□ ON **2023-05-26 04:04:51**

Hello,

We're still waiting and asking for the usage of access key in the response data. We may confirmed all info we need and reply to you in May.

Company's number, address, postal (may) is also public information and can be searched using search engine or government public search system to let customer to know the info. In legal affair, if customer want to prosecute seller when they have civil dispute, the plaintiff should give the court the contact info of the accused to mail the indictment.

Best Regards.

ADITYASHENDE ON **2023-05-26 04:38:59**

Let me know if you get reply from team. I am trying to escalate more but now as it’s patched I can’t do much more

ADITYASHENDE ON **2023-06-03 10:51:15**

Any updates on bounty ?

I can see the bug has been patched but also the data can be viewed via https://web.archive.org/web/20230309234636/https://mkpdata.huaweicloud.com/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/efc3aa0c2b7da6f10e377d52b44547ba/info

ADITYASHENDE ON **2023-06-06 07:41:48**

Hello team,
The bug has been patched.

□□□□□□□□ ON **2023-06-09 04:26:09**

Updated the CVSS score.

Score	9.8 → 5.3
Severity	Critical → Medium

□□□□□□□□□ ON 2023-06-09 04:29:42

Hello,

We've confirm all the data field from the development team, there is only a sensitive data field which is access_key. But this access_key can not be used independently and the APIs which use access_key do not leak sensitive or user private data.

Your report is therefore eligible for a reward – stay tuned.
Congrats.

□□□□□□□□□ ON 2023-06-09 04:29:58

UNDER REVIEW → **ACCEPTED**

ADITYASHENDE ON 2023-06-30 08:22:24

Hey team ,

Any updates on bounty ?

□□□□□□□□□ ON 2023-07-13 08:49:48

€200.00 and **7 pts** rewarded to **ADITYASHENDE**

Congratulations!

According to the resolution of the HUAWEI CLOUD Bug Bounty Review Team, we'll give €200 bonus including €100 April double activity bonus to you.

Happy Hunting!

ADITYASHENDE ON 2023-07-13 09:41:39

So it should be 300 right?

□□□□□□□□□ ON 2023-08-31 10:54:06

Hello,

The basic bounty is €100, and the activity will double it to €200. So, we would give you €200 bounty in total.

Regards.

□□□□□□□□□ ON **2023-08-31 10:54:13**

ACCEPTED → INFORMATIVE