YES WE HACK

#YWH-PGM2368-95 UNDER REVIEW

/ IDOR disclosing PII information via enumerating ISV ID through JSON response

HUAWEI CLOUD BUG BOUNTY PROGRAM

SUBMITTED BY ADITYASHENDE ON 2023-04-30

REPORT DETAILS

BUG TYPE	Insecure Direct Object Reference (IDOR) (CWE-639)
SCOPE	*.huaweicloud.com (including *.huaweicloud.com/intl/)
ENDPOINT	/api/marketplace/adapt/v1/portal/product/query?forms=§1104§
SEVERITY	Critical
VULNERABLE PART	get-parameter
PART NAME	forms=
PAYLOAD	0000 to 999
TECHNICAL ENVIRONMENT	Ubuntu
APPLICATION FINGERPRINT	
IP USED	152.57.242.74

CVSS SCORE	SEVERITY
10	CRITICAL

VECTOR STRING

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

BUG DESCRIPTION

Summary:

The URL https://mkpdata-intl.huaweicloud.com/api/marketplace/adapt/v1/portal/product/query?forms=1104&page=1 is vulnerable to an information disclosure vulnerability. Specifically, the "forms" parameter is vulnerable, as it is revealing the ISV ID in an encoded form, which in turn is disclosing business information.

Impact:

The impact of this vulnerability is that it is exposing sensitive information that could be used by attackers to target specific businesses or individuals. In particular, the ISV ID is being revealed, which could be used to identify the specific vendor of the product, which may be sensitive information that the vendor would not want to be publicly disclosed.

Steps to Reproduce:

Go to the URL https://mkpdata-intl.huaweicloud.com/api/marketplace/adapt/v1/portal/product/query?forms=1104&page=1
Observe that the ISV ID is being revealed in an encoded form.
Decode the ISV ID and observe that it is disclosing business information.
Recommended Solution:

The recommended solution is to remove the vulnerability by modifying the code to not reveal the ISV ID or any other sensitive information. This can be achieved by encoding the sensitive information in a way that it cannot be easily decoded, or by removing it altogether.

In addition, the website owners should review their security protocols and implement appropriate measures to prevent future vulnerabilities.

Bug Chain

EXPLOIT CHAIN BUG ID #YWH-PGM2368-93

PII Data Exposure in https://mkpdata.huaweicloud.com/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/68bcb36dcc3b41ca880d92f36422fa0e/info

Summary:

The URL https://mkpdata.huaweicloud.com/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/68bcb36dcc3b41ca880d92f36422fa0e/info is vulnerable to a PII (Personally Identifiable Information) data exposure vulnerability. Specifically, the ISV ID is being used as a parameter in the URL, which is revealing sensitive information such as PII data.

Impact:

The impact of this vulnerability is that it is exposing sensitive PII data that could be used by attackers for malicious purposes such as identity theft or fraud. This vulnerability is particularly dangerous as the PII data could belong to the customers or users of the affected business.

Steps to Reproduce:

Copy the URL
https://mkpdata.huaweicloud.com/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/68bcb36dcc3b41ca880d92f36422fa0e/info
Add the ISV ID of the desired business as a parameter in the URL.
Access the modified URL and observe that it is revealing sensitive PII data.

COMMENTS

ADITYASHENDE ON 2023-04-30 12:10:13

NEW

□□□□□□□□ ON 2023-05-09 07:47:42

NEW → UNDER REVIEW

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

□□□□□□□□ ON 2023-05-25 08:05:56

Hello,

This API is also in your YWH-PGM2368-93 report, we would like to ask if 93 and 95 are not the same issue? If we do not misunderstand it and they are the same issue. We will close this report with RTFS status so you will not lose your point and track this issue in report 93.

Best Regards.

ADITYASHENDE ON 2023-05-25 08:24:35

With all due respect 93 and 95 bugs aren’t same . I escalated issue by enumeration if ISV ID to get more information disclosure and it worked . i can explain more if you want. But please make sure to count in different manner I’ve other way to bypass so I can craft that report too . Happy to help more

ADITYASHENDE ON 2023-05-25 10:49:23

In report 95 I did idor on https://mkpdata-intl.huaweicloud.com/api/marketplace/adapt/v1/portal/product/query?forms=1104&page=1 [ON forms parameter which was disclosing isv id , So I escalated it with report 95 where I put ISV ID after this url : https://mkpdata.huaweicloud.com/api/marketplace/global/rest/cbc/cbcmarketplaceisvmgmntservice/v1/isv/ISV_ID_HERE/info

This was disclosing more information. I do believe this escalation is good more to understand

ADITYASHENDE ON 2023-06-06 07:42:38

this vulnerability is also patched which is escalated in 93 and 95

ADITYASHENDE ON 2023-06-30 08:23:37

Can you share updates on this as 93 and 95 are chained ?