

YES WE H/CK

#YWH-PGM2368-101

RTFS

## / Information Disclosure in CBC Marketplace Comment Service

HUAWEI CLOUD BUG BOUNTY PROGRAM

SUBMITTED BY ADITYASHENDE ON 2023-05-22

### REPORT DETAILS

BUG TYPE	Business Logic Errors (CWE-840)
SCOPE	*.huaweicloud.com (including *.huaweicloud.com/intl/)
ENDPOINT	/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering_id=13df60e0-6a6e-4e2a-8775-55dbca5b0ff0&offset=0&limit=50
SEVERITY	Critical
VULNERABLE PART	get-parameter
PART NAME	offering_id=13df60e0-6a6e-4e2a-8775-55dbca5b0ff0&offset=0&limit=50
PAYLOAD	/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering_id=UUID_here&offset=0&limit=50
TECHNICAL ENVIRONMENT	Ubuntu WSL
APPLICATION FINGERPRINT	
IP USED	43.241.25.178

### CVSS SCORE

10

### SEVERITY

CRITICAL

### VECTOR STRING

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

## BUG DESCRIPTION

### Summary:

A vulnerability has been identified in the CBC Marketplace Comment Service, which allows unauthorized users to access sensitive information such as user answers and comments, as well as extract UUIDs and encrypted IDs. This vulnerability can be exploited by manipulating the URL parameters in the API endpoint.

### Vulnerability Details:

The vulnerability exists in the CBC Marketplace Comment Service API, specifically in the "question/all" endpoint. By manipulating the "offering\_id" parameter, an attacker can retrieve user answers and comments without proper authorization. Additionally, the UUIDs and encrypted IDs associated with the comments can also be extracted.

### Exploit Code:

The following Bash code demonstrates how the vulnerability can be exploited:

```
/ !/bin/bash
```

```
URL="https://web.archive.org/cdx/search/cdx?url=*.mkpdata.huaweicloud.com&output=text&fl=original&collapse=urlkey"
OUTPUT_FILE="uuid.txt"
```

/ Curl the URL, grep UUIDs, and save them in the output

file

```
curl_output=$(curl -s "$URL" | grep -oE '\b[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}\b')
echo "$curl_output" > "$OUTPUT_FILE"

echo "UUIDs saved in $OUTPUT_FILE"
```

Impact:  
This vulnerability exposes sensitive user information, including their answers and comments, which may contain personally identifiable information (PII) or confidential data. Additionally, the extraction of UUIDs and encrypted IDs can potentially be leveraged for further attacks or unauthorized access to the system.


Recommended Actions:

Implement proper access controls and authentication mechanisms to restrict access to user answers and comments.  
Apply input validation and sanitization techniques to prevent manipulation of URL parameters.  
Encrypt or obfuscate sensitive information stored in the CBC Marketplace Comment Service database.  
Regularly monitor and log API requests to detect any unauthorized access attempts.  
Mitigation:  
We recommend applying the following measures to mitigate the identified vulnerability:


Conduct a thorough code review of the CBC Marketplace Comment Service to identify any other potential information disclosure vulnerabilities.  
Implement a robust authentication and authorization system that ensures only authorized users can access user answers and comments.  
Encrypt or tokenize sensitive data stored in the CBC Marketplace Comment Service database to protect against unauthorized extraction.  
Regularly update and patch the CBC Marketplace Comment Service to address any security vulnerabilities.

URLs:  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=42a16d27-db96-407d-a756-76d8fdc92313&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=4cc2f496-e36e-47ba-8d90-abbbdc23cdda&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=5b47c46d-df58-471e-b64c-14d47d75d295&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=eba284cb-7c6a-42af-a3d2-44a6f695c93e&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=e1ff556d-a43c-4535-97e5-19de7709d806&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=5175e9bc-e1e1-4243-ac3f-45a81f6980f7&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=ef750023-f243-4bea-8f59-d059b6bddcbf&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=6c8a375a-4cdf-40c7-b7b6-4af9173f9e16&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=817ab039-aff1-4edd-917d-f64c5ffc992d&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=0cadf157-b54f-43b1-b94b-e56c1fda3c8f&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=0cadf157-b54f-43b1-b94b-e56c1fda3c8f&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=e11b9137-bd1c-4dbb-8ae5-afb44f1e244&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=e11b9137-bd1c-4dbb-8ae5-afb44f1e244&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=13df60e0-6a6e-4e2a-8775-55dbca5b0ff0&offset=0&limit=50  
https://mkpdata.huaweicloud.com/rest/rest/cbc/cbcmarketplacecommentsservice/v1/question/all?offering\_id=13df60e0-6a6e-4e2a-8775-55dbca5b0ff0&offset=0&limit=50

COMMENTS



**ADITYASHENDE ON 2023-05-22 12:57:59**

**NEW**



ADITYASHENDE ON 2023-05-22 12:58:45



Bash code : #!/bin/bash

URL="https://web.archive.org/cdx/search/cdx?

url=\*.mkpdata.huaweicloud.com&output=text&fl=original&collapse=urlkey"

OUTPUT\_FILE="uuid.txt"

## / Curl the URL, grep UUIDs, and save them in the output file

```
curl_output=$(curl -s "$URL" | grep -oE '\b[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}\b')  
echo "$curl_output" > "$OUTPUT_FILE"
```

```
echo "UUIDs saved in $OUTPUT_FILE"
```



██████████ ON 2023-05-25 07:49:48



NEW



UNDER REVIEW



Hello,

Thanks for your submission

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

Regards.



██████████ ON 2023-06-06 05:47:33



Hello,

Thanks for your submission on our program.

This API is used for get Q&A content in Huawei Cloud Store Product Page, the content is open to all users(like <https://marketplace.huaweicloud.com/contents/79087d0f-43d9-4a7e-8ab2-9f3f1ad1d752#productid=OFFI826753763787939840>, Q&A is in the bottom), it do not have Information Leak issue.

Unfortunately, we cannot consider your report as valid, based on our program's rules.

You report will be closed with status 'RTFS', so that you don't loose ranking points.

We hope that you will keep on participating in our program and we wish you better luck in your next findings.

Regards.



██████████ ON 2023-06-09 03:47:25



UNDER REVIEW



RTFS