#YWH-PGM2368-97 RTFS

/ Data Exposure on Obs-shlife-website-prd.obs.cn-east-201.jrzq.huaweicloud.com

HUAWEI CLOUD BUG BOUNTY PROGRAM

SUBMITTED BY ADITYASHENDE ON 2023-05-14

REPORT DETAILS

BUG TYPE	Information Disclosure (CWE-200)
SCOPE	*.huaweicloud.com (including *.huaweicloud.com/intl/)
ENDPOINT	/productConfig/%E4%BE%9B%E5%BA%94%E5%95%86%E5%88%97%E8%A1%A8.xlsx?AWSAccessKeyId=EMCIXMV4QDOLMO22UVRG&Expires=1817712721&Signature=iZPyLyfOIlFriAlEy5Zrdr%2FdBsw%3D i
SEVERITY	Critical
VULNERABLE PART	get-parameter
PART NAME	/productConfig/%E4%BE%9B%E5%BA%94%E5%95%86%E5%88%97%E8%A1%A8.xlsx?AWSAccessKeyId=EMCIXMV4QDOLMO22UVRG&Expires=1817712721&Signature=iZPyLyfOIlFriAlEy5Zrdr%2FdBsw%3D i
PAYLOAD	/productConfig/%E4%BE%9B%E5%BA%94%E5%95%86%E5%88%97%E8%A1%A8.xlsx?AWSAccessKeyId=EMCIXMV4QDOLMO22UVRG&Expires=1817712721&Signature=iZPyLyfOIlFriAlEy5Zrdr%2FdBsw%3D i
TECHNICAL ENVIRONMENT	Win10
APPLICATION FINGERPRINT	
IP USED	152.58.17.88

CVSS SCORE	SEVERITY
9.8	CRITICAL

VECTOR STRING

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

BUG DESCRIPTION

Description: The URL https://obs-shlife-website-prd.obs.cn-east-201.jrzq.huaweicloud.com/productConfig/%E4%BE%9B%E5%BA%94%E5%95%86%E5%88%97%E8%A1%A8.xlsx?AWSAccessKeyId=EMCIXMV4QDOLMO22UVRG&Expires=1817712721&Signature=iZPyLyfOIlFriAlEy5Zrdr%2FdBsw%3D is exposing sensitive data related to Cooperating Organization Name, Contact Information, Processing Purpose, Processing Method, and Type of Personal Information. This is a serious security vulnerability that could potentially lead to the compromise of personal information and the privacy of individuals.

Impact: The exposure of sensitive data related to Cooperating Organization Name, Contact Information, Processing Purpose, Processing Method, and Type of

Personal Information can lead to identity theft, fraud, and other malicious activities. This could have a significant impact on the individuals whose data is exposed, as well as the reputation and legal liability of the organization responsible for the data.

Steps to Reproduce:

Visit the URL: https://obs-shlife-website-prd.obs.cn-east-201.jrzq.huaweicloud.com/productConfig/%E4%BE%9B%E5%BA%94%E5%95%86%E5%88%97%E8%A1%A8.xlsx?AWSAccessKeyId=EMCIXMV4QDOLMO22UVRG&Expires=1817712721&Signature=iZPyLyfOIlFriAlEy5Zrdr%2FdBsw%3D
The sensitive data related to Cooperating Organization Name, Contact Information, Processing Purpose, Processing Method, and Type of Personal Information will be visible.

Recommendation: The organization responsible for the website should immediately address this vulnerability by implementing access controls, encryption, and other security measures to protect the sensitive data from unauthorized access. It is also recommended that the organization conducts a thorough security audit to ensure that no other vulnerabilities exist on their website or related systems.

COMMENTS

ADITYASHENDE ON 2023-05-14 15:31:38

NEW

□□□□□□□□ ON 2023-05-17 08:13:29

NEW → UNDER REVIEW

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

□□□□□□□□ ON 2023-06-14 05:08:00

UNDER REVIEW → RTFS

Hello,
Thanks for your first submission on our program.
This OBS URL belongs to Huawei Cloud outter tenant. Unfortunately, we cannot consider your report as valid, based on our program’s rules.
You report is 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.