#YWH-PGM2368-118 INVALID

/ Configuration File Source Code Disclosure via .zip File and app secrets, app IDs, internal IP addresses, and Java JAR code exposure

HUAWEI CLOUD BUG BOUNTY PROGRAM

SUBMITTED BY ADITYASHENDE ON 2023-07-27

REPORT DETAILS

BUG TYPE	Information Exposure Through Directory Listing (CWE-548)
SCOPE	*.huaweicloud.com (including *.huaweicloud.com/intl/)
ENDPOINT	/upload/files/sdk
SEVERITY	Critical
VULNERABLE PART	path
PART NAME	static.huaweicloud.com/upload/files/sdk
PAYLOAD	static.huaweicloud.com/upload/files/sdk/enpoint_here
TECHNICAL ENVIRONMENT	Windows 10 , Chrome
APPLICATION FINGERPRINT	
IP USED	45.115.58.138

CVSS SCORE	SEVERITY
9.4	CRITICAL

VECTOR STRING

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

BUG DESCRIPTION

Vulnerability Description:
The issue resides in the .zip files mentioned above, which contain sensitive configuration files, including app secrets, app IDs, internal IP addresses, and Java JAR code URLs. These files should not be publicly accessible, as they can provide attackers with valuable information to exploit the application and gain unauthorized access to internal resources. The presence of such sensitive data in publically accessible archives poses a significant risk to your organization's security.

Steps to Reproduce:
To reproduce the issue, follow these steps:

Download the affected .zip file from the provided URLs.
Extract the contents of the .zip file using standard archive extraction tools.
Analyze the extracted files to find sensitive configuration files containing app secrets, app IDs, internal IP addresses, and Java JAR code URLs.

NOTE :

1. https://static.huaweicloud.com/upload/files/sdk/OceanConnectJava_1561428097.zip
2. Extract it : Go to OceanConnectJava_1561428097
3. Open config.properties

Data :
platformIp=100.115.191.110
platformPort=8743
appId=bohmsGlAElm_oeJVnpnDvNB7ffMa
secret=d5VB20n7s_OecAqpHXVVCmChctMa

There are also other folders which are disclosing pem certs and demo TCP requests POST with partial access_tokens

Attacker can gather much more information to lavarage issue

Impact:
An attacker with knowledge of these URLs and sensitive information could potentially compromise the integrity and confidentiality of your services. The disclosure of app secrets and app IDs could lead to unauthorized access to user data, unauthorized API calls, and potential financial losses. Additionally, the exposure of internal IP addresses may allow attackers to launch targeted attacks against your internal infrastructure, leading to service disruptions or unauthorized access to critical resources.

Recommendations:

To address this issue and enhance the security of your system, I recommend the following actions:

Immediate: Remove the affected .zip files from the provided URLs to prevent further exposure of sensitive data.
Review all files hosted on your domain for sensitive information leakage and limit public access to configuration files that contain sensitive data.
Regularly audit and scan your systems for potential security vulnerabilities, including source code disclosure and sensitive data exposure.
Implement access controls and authentication mechanisms to restrict access to sensitive files and directories.
Encourage responsible disclosure by providing a clear and straightforward bug bounty program, which incentivizes security researchers to report vulnerabilities.

COMMENTS

ADITYASHENDE ON 2023-07-27 15:14:13

NEW

□□□□□□□□ ON 2023-07-28 05:31:17

NEW → UNDER REVIEW

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

□□□□□□□□ ON 2023-08-04 09:26:51

UNDER REVIEW → INVALID

Dear,

That ZIP file is not sensitive information, it's a DEMO file, not a PRODUCT environment.

Best Regards