Bucket "h2o-release" publicly writable, allowing an attacker to replace any file in h2oai/h2o-3

✓ Valid Reported on Jan 26th 2025

The S3 bucket "h2o-release" where you host docs and which you instruct your users to use as a Maven repo (e.g. in here https://github.com/h2oai/h2o-3?tab=readme-ov-file#3-using-h2o-3-artifacts) is publicly writable. It is possible to overwrite any file in that bucket.

As a PoC I created the following file: https://s3.amazonaws.com/h2o-release/h2o-3-deep-freeze/anqi-gbm/1/Rjar/h2o.jar.poc I didn't want to overwrite any existing file to not disturb real users, but that is still possible.

Here is curl command to write to the bucket:

```
curl -H "Content-Type: text/plain" -i -X PUT 'https://s3.amazonaws.com/h2o-release/h2o-
```

Impact

As users are downloading binary files (like JARs) from the bucket it will lead to RCE on any user who uses this application. Furthermore, an attacker could alter the documentation to contain download links to attacker's own website.

We are processing your report and will contact the **h2oai/h2o-3** team within 24 hours. 3 months ago

huntr-helper commented 3 months ago Admin

This report was determined to possibly be out of scope or have a high likelyhood of being marked as informative.

Please review your report and the Participation Guidelines.

These are the specific guidelines this report is in possible violation of:

- Non-code level (e.g. network or physical) vulnerabilities

Adam Valenta validated this vulnerability 3 months ago

Fixed

minecraft237 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

CVE-2025-0782 assigned to this report. 3 months ago

Adam Valenta marked this as fixed in Fixed by DevOps in aws config with commit 674065 3 months ago

The fix bounty has been dropped ✕

Michal Malohlava commented 3 months ago Maintainer

Not reproducible:

```
❯ curl -H "Content-Type: text/plain" -i -X PUT 'https://s3.amazonaws.com/h2o-release/h2o-3-deep-free

HTTP/1.1 403 Forbidden
x-amz-request-id: 0HA73JCPPDMZ00SQ
x-amz-id-2: chAfic/LxqDrkwS+S55tHd7+KVqJncD6NgOJwv+PpvWgvyzLOf2KHbmomDbJu7r0w4oUyi0MFjU=
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 11 Feb 2025 00:52:39 GMT
Connection: close
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<Error><Code>AccessDenied</Code><Message>Access Denied</Message><RequestId>0HA73JCPPDMZ00SQ</Request
```

A h2oai/h2o-3 maintainer has acknowledged this report 3 months ago

The scheduled publication date was automatically extended from 26th Apr 2025 to 3rd May 2025 due to the maintainers acknowledgement of the report 3 months ago

Michal Malohlava commented a month ago Maintainer

Fixed in AWS setup:

```
❯ curl -H "Content-Type: text/plain" -i -X PUT 'https://s3.amazonaws.com/h2o-release/h2o-3-deep-free
```

```
HTTP/1.1 403 Forbidden
x-amz-request-id: ATYX7FNNKGEXAKZ6
x-amz-id-2: ja46LEreeF5NSPODyQFMw7H88NkODviWy8pxUFj0apMHtHWpgVuLyBvj9/DRuIb+9D8lP23Qr7Y=
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Thu, 27 Mar 2025 20:37:21 GMT
Connection: close
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<Error><Code>AccessDenied</Code><Message>Access Denied</Message><RequestId>ATYX7FNNKGEXAKZ6</Request
```

minecraft237 commented a month ago Researcher

If it's not eligible for bounty, then please let's also not disclose it publicly.

We have notified the **h2oai/h2o-3** maintainers about this report in their weekly follow-up 5 days ago

We have sent a warning to the **h2oai/h2o-3** team to inform them that this report will be published in 48 hours 3 days ago

Michal Malohlava commented 3 days ago Maintainer

> We have sent a warning to the h2oai/h2o-3 team to inform them that this report will be published in 48 hours

Why it is published ? It is fixed and it is not product issue.

This vulnerability has now been published 21 hours ago

CVE-2025-0782 has now been published 21 hours ago

Sign in to join this conversation

CVE
CVE-2025-0782
(Published, Under Review)

Vulnerability Type
CWE-862: Missing Authorization

Severity
Critical (10)

Attack vector	Network

Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	None

Open in visual CVSS calculator

Registry

Other

Affected Version

all

Visibility

Public

Status

Fixed

Found by

minecraft237

@minecraft237

UNPROVEN

Supported by Protect AI and leading the way to MLSecOps and greater AI security.

Privacy Policy Terms of Service Code of Conduct Cookie Preferences Contact Us