

PDF Export for report 3126108

Subdomain takeover offliptop.zendesk.com from developer.fliptop.com(business.linkedin.com)

State	Triaged
Reported by	S.Lakshmi Vignesh (w3shi)
Reported to	LinkedIn (linkedin)
Submitted at	2025-05-04T14:10:28.338Z (ISO-8601)
Asset	business.linkedin.com (URL)
References	
Weakness	
Severity	Low (2.4) []
CVE IDs	

Greetings Security Team,

Fliptop.com is a acquisition of linkedin, The users requests are automatically redirected to business.linkedin.com and all the subdomain are redirected too except developer.fliptop.com.

and in developer.fliptop.com the Support/FAQs domain fliptop.zendesk.com is vulnerable to takeover. Attacker can takeover this domain and distribute malicious or false content.

Steps to Reproduce:

- 1.go to developer.fliptop.com
1. Click on Submit Request or Support

{F4314062}

- 3.You could observe the following takeover

{F4314065}

{F4314069}

Impact

Malware Distribution: Malicious files or software could be hosted on the subdomain, infecting visitors' devices with malware when they access the compromised subdomain.

Data Breach: If the subdomain hosts sensitive data or services, a takeover could lead to a data breach, exposing confidential information to unauthorized parties.

Phishing Attacks: Attackers could create phishing pages on the hijacked subdomain, impersonating legitimate websites to steal sensitive information like login credentials, credit card details, etc

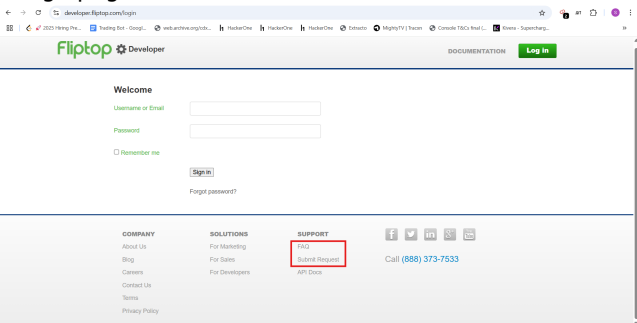


image.png

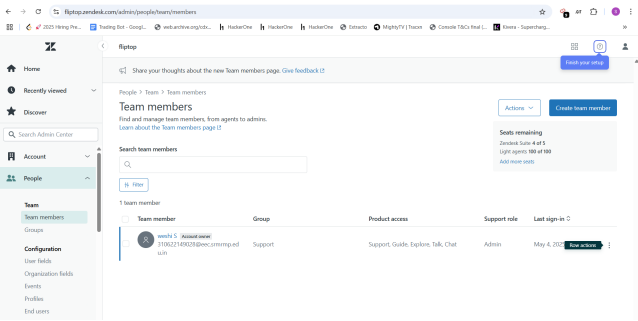
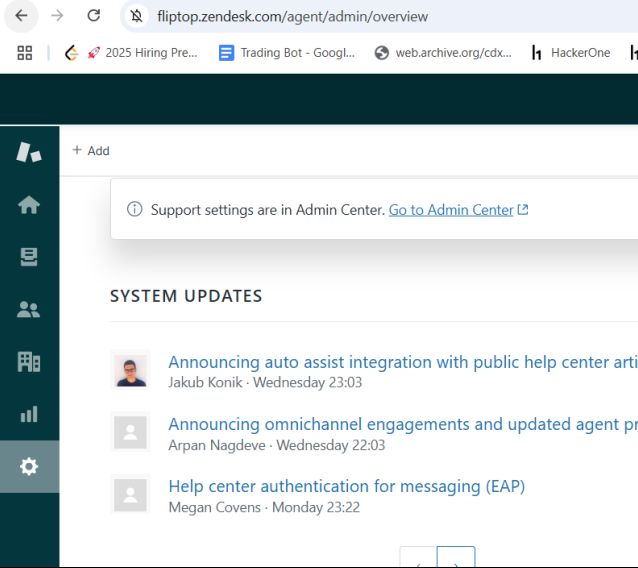


image.png



Activity

Greetings @linkedin,

The subdomain `http://developer.flippot.com/` was taken down and I can confirm the vulnerability is fixed with that!.

Warm Regards

w3shi

	2025-07-10 11:09	comment	Public
--	------------------	---------	--------

greetings @linkedin, @aashna_sethi

Thank you for the bounty!, Appreciate it

Looking forward to contribute again

Thank you & regards

W3shi(S.Lakshmi Vignesh)

	2025-06-07 08:21	comment	Public
	2025-06-06 19:55	bounty awarded	Public
	2025-06-06 19:55	bounty awarded	Public

Hello @w3shi,

I hope all is well and thanks for leaving a message.

Please refrain from updating the report. We detailed that we will give you an update when we have one to share.

Thanks and regards,

@h1_analyst_jack

2025-06-03 22:51	comment	Public
<p>greetings @linkedin, @aashna_sethi</p> <p>I understand that the team is handling numerous reports. But I'd appreciate an update on the issue if any.</p> <p>Thank you & regards</p> <p>W3shi</p>		
2025-06-03 14:22	comment	Public
<p>greetings @linkedin,</p> <p>I understand that the team is handling numerous reports. But I'd appreciate an update on the issue if any.</p> <p>Thank you & regards</p> <p>W3shi</p>		
2025-05-30 10:05	comment	Public
<p>greetings @linkedin,</p> <p>I understand that the team is handling numerous reports. But I'd appreciate an update on the issue if any.</p> <p>Thank you & regards</p> <p>W3shi</p>		
2025-05-25 17:25	comment	Public
<p>Hello @w3shi,</p> <p>I hope all is well and thanks for leaving a message.</p> <p>Please remain patient. The LinkedIn team will update the report when they have one to provide.</p> <p>Thanks and regards,</p> <p>@h1_analyst_jack</p>		
2025-05-20 05:43	comment	Public
<p>greetings @aashna_sethi , @linkedin, @h1_analyst_jack ,</p> <p>I understand that the team is handling numerous reports. But I'd appreciate an update on the issue if any.</p> <p>Thank you & regards</p> <p>W3shi</p>		
2025-05-20 04:50	comment	Public
<p>greetings @aashna_sethi , @linkedin, @h1_analyst_jack ,</p> <p>I understand that the team is handling numerous reports. But I'd appreciate an update on the issue if any.</p> <p>Thank you & regards</p> <p>W3shi</p>		
2025-05-18 07:20	comment	Public
<p>greetings @aashna_sethi , @linkedin, @h1_analyst_jack ,</p> <p>I understand that the team is handling numerous reports. But I'd appreciate an update on the issue if any.</p> <p>Thank you & regards</p> <p>W3shi</p>		
2025-05-15 17:52	comment	Public
<p>greetings @aashna_sethi , @linkedin,</p>		

I understand that the team is handling numerous reports. But I'd appreciate an update on the issue if any.

Thank you & regards
W3shi

2025-05-13 19:24	comment	Public
2025-05-06 20:41	bug triaged	Public

Hello @w3shi,

Thank you for your submission! We were able to validate your report, and have submitted it to the appropriate remediation team for review. They will let us know the final ruling on this report, and when/if a fix will be implemented. Please note that the status and severity are subject to change.

Thanks,
@h1_analyst_jack

2025-05-05 06:14	bug pending program review	Public
2025-05-05 06:13	report severity updated	Public

Greetings @h1_analyst_jack ,

Thanks for asking,

{F4314065}

Here you could observe that I've taken the ownership of Fliptop.zendesk.com which was already provided.

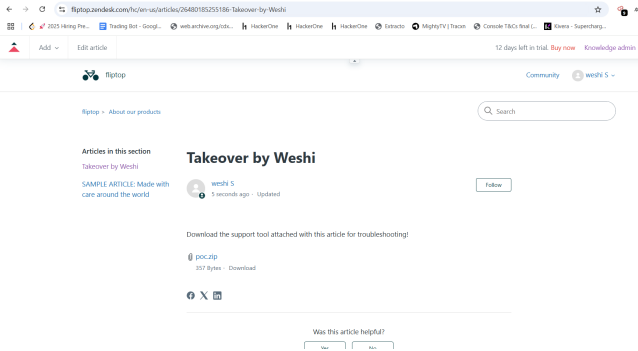
Now I've modified the content of Support instance which you could observe by going to this link

<https://fliptop.zendesk.com/hc/en-us/articles/26480185255186-Takeover-by-Weshi>

{F4315490}

Best Regards
W3shi

image.png



2025-05-05 04:15	bug new	Public
------------------	---------	--------

Hello @w3shi,

I hope all is well and thanks for leaving a message.

Where is the PoC page I can visit and see? There does not seem to be any impact to this because I do not see a PoC page where you can even try to dupe a victim into downloading malware.

Thanks and regards,
@h1_analyst_jack

2025-05-04 22:16	bug needs more info	Public
------------------	---------------------	--------

2025-05-04 17:35	report collaborator joined	Public
------------------	----------------------------	--------

2025-05-04 16:09	report collaborator invited	Public
------------------	-----------------------------	--------

Greetings @h1_analyst_jack ,

The Support Domain of fliptop.com is directly hosted in Fliptop.zendesk.com,Which you could observe in Developer.fliptop.com.

Warm regards
W3shi(S.Lakshmi Vignesh)

2025-05-04 16:09	bug new	Public
------------------	---------	--------

Hello @w3shi,

I hope all is well and thanks for leaving a message.

Can you demonstrate the subdomain takeover in the DNS Name of LinkedIn? The DNS takeover in the name of ZenDesk is not so impactful to LinkedIn.

Thanks and regards,
@h1_analyst_jack

2025-05-04 15:44	bug needs more info	Public
------------------	---------------------	--------

2025-05-04 14:10	report vulnerability information updated	Public
------------------	---	--------