LinkedIn Vulnerability Report

Inbox x

SHREATEH <@gmail.com>

Nov 20

to security

Dear LinkedIn Security Team,

My name is Khalil Shreateh, and before i start i wanna tell that i followed your Hackerone profile information : https://hackerone.com/linkedin that so i hope this is the best place to report a vulnerability.

Vulnerability Description:

- Attacker can get any Linkedin user private IP address, Browser User Agent, HTTP REFERER ... etc

- Vulnerability can be exploited by modifying the SRC value for the uploaded image by the attacker.

- Exploit will be triggered soon as linkedin user clicked the image .

Vulnerability Discovery

- Discovered manually without using any automated tools.

Exploitation

- To exploit this vulnerability attacker need to submit and XHR request to : (https://www.linkedin.com/voyager/api/feed/shares?action=create) which is the scope of creating new post. With a modified value of the variable : url
- The "url" variable is the SRC attribute of the uploaded image.
- Modify "url" value to remote PHP file hosted out side linkedin. That so attacker can get user's details soon as the image will be clicked.

Please check attached pictures (1-3).

3 Attachments

Sanjay Parab **<sparab@linkedin.com>** Nov 20

to me

Hi Khalil,

Thank you for your report. We will investigate it and get a response back to you when we have completed our analysis.

Regards,
Sanjay

From: SHREATEH <@gmail.com>
Date: Monday, November 20, 2017 at 5:19 AM
To: security <security@linkedin.com>
Subject: LinkedIn Vulnerability Report

SHREATEH **<@gmail.com>** Nov 22

to Sanjay

hi Sanjay ,

please check the attached picture, vulnerability escalated to steal linkedin users credentials by using WWW-Authenticate

thanks

Attachments area

Sanjay Parab Nov 25

to me

Hi Khali,

Thanks for reaching out to us.
After careful consideration of your report, we believe this does not represent security vulnerability as it requires explicit user interaction.

It is similar to someone sending phishing email. Alternatively, each of the LinkedIn member can request any post to be marked as spam via using "Report this post" feature.

That being said, if you could find a way to automatically trigger code execution on user's browser, please write to us and we will investigate your report.

Regards,
Sanjay

From: SHREATEH <@gmail.com>
Date: Wednesday, November 22, 2017 at 3:39 AM
To: Sanjay Parab <sparab@linkedin.com>
Subject: Re: LinkedIn Vulnerability Report

SHREATEH <@gmail.com>

Nov 25

to Sanjay

hi sanjay,

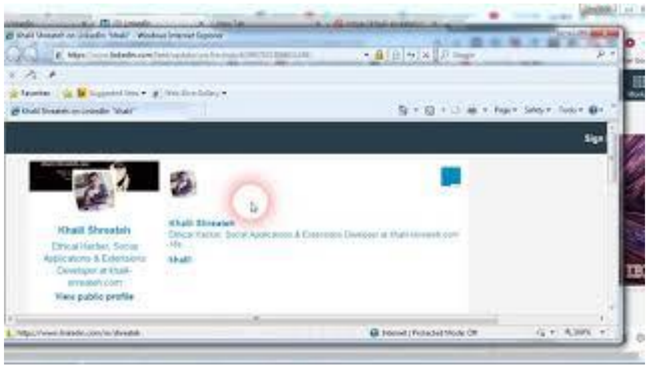
actually it works without any interaction of any user, even it works for non-logged in users.

To demonstrate this exploit follow my previous report then check the LinkedIn post from internet explorer on PC (and there is many other browsers) .
also check it from chrome browser app on mobile (latest version) (and there is many other browsers)

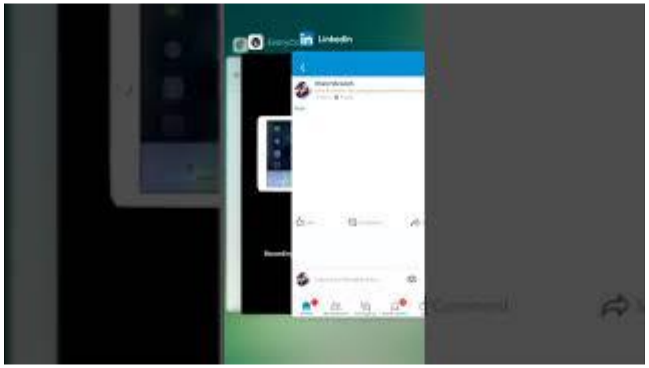
anyway here is a POC videos:

- POC on PC via internet explorer : https://youtu.be/cCX7mhcG5BY
- POC on mobile via chrome (latest version), Dolphin (latest version): https://youtu.be/IKvbPf1KXV0

Attachments area
Preview YouTube video PC LinkedIn exploit POC 1


Favorites
Khalil Shreateh on LinkedIn: "khalil"
Page ▾ Safety ▾ Tools ▾
Sign
Khalil Shreateh
Ethical Hacker, Social Applications & Extensions Developer at khalil-shreateh.com
View public profile
Khalil Shreateh
khalil
Internet | Protected Mode: Off

Preview YouTube video mobile LinkedIn exploit #2



Sanjay Parab Nov 27

to me

Hi Khalil,

Thanks for sending additional information. I reviewed videos you shared. However, user still has to copy the url of your post and put in Chrome/IE browser. As this requires user interaction, we believe this does not represent security vulnerability

If you believe there is another way which does not requires user interaction, please write to us.

Regards,
Sanjay

From: SHREATEH <@gmail.com>
Sent: Friday, November 24, 2017 10:47 PM
To: Sanjay Parab

SHREATEH **<@gmail.com>** Nov 27

to Sanjay

hi sanjay,

i think you msitake my POC videos, here is the full scenario :

- attacker create new post and insert www-authenticate via that exploit in image SRC attribute.
- linkedin shows the video for all attacker's connections.
- each linkedin connection will be hacked soon as the post appears on his newsFeed, for all linkedin users who uses linkedin on:

- Windows explorer browser (and there is many others).
- Chrome browser on mobile (and there is other browsers as the POC shows) .

in the previous POC videos i copied the link cause i used my same linkedin account.

however i can create a new linkedin account and show you another POC video without user interaction.

thank you for understanding.

SHREATEH **<@gmail.com>**

Nov 27

to Sanjay

hi sanjay,

sorry i did not noticed that when creating POC video in first 2 parts that i was not logged in to linkedin.

however, this is another demonstration POC video, please confirm that linkedin security team doesnt recognize it as a security issue.

Scenario:
- Attacker create a new post, post will contain image contains video play thumbnail.
- Any user who will click on that post will be hacked (Auto collect IP Address and other user details, Linkedin credentials if inserted)
YOUTUBE UNLISTED POC VIDEO : https://youtu.be/WEie-Tpgz4E

Thank you .

Attachments area

Preview YouTube video Linkedin Exploit POC #3

SHREATEH <@gmail.com>

Nov 27

to Sanjay

hi sanjay,

Beside my last email for you, i believe that its a high risk security issue because attacker can use linkedin platforms to steal any person private information (IP ADRESS AND MORE) ,
 even if the target person is not logged in to linkedin, simply by sending the direct post link via email as i show in first 2 poc videos,
however there is no need to copy and paste into any browser while using mobile or internet explorer on PC. the exploit works on most of mobile mail client applications,
 i used MyMail app : https://itunes.apple.com/us/app/mymail-email-app/id722120997?mt=8

many thanks

Sanjay Parab

Nov 28

to me

Hi Khalil ,

Could you please send url of your PoC ? I believe you are creating post with image content in it and modifying image url to point to evil domain.

Let me know, if this is not the case.

Regards,
Sanjay

From: SHREATEH <@gmail.com>
Date: Sunday, November 26, 2017 at 10:17 PM

khalil shreateh <@gmail.com>

Nov 28

to Sanjay

Hi sanjay,

Thats true and that is the main point in my report as also the POC's video show.

I will forward you a direct link to a post, with all info needed. But i want you to know and agree with 2 things:
- this will be upon linkedin request and no harmful action will be taken from my side as the post will appear on my linkedin connections till you confirm back to delete it.
- second i will use my own website, that so i make sure we will stay in close circle to avoid any invalid traffic or anything else to others.

Please confirm back to create and send you a POC post link.

Thanks

Sent from myMail for iOS

Tuesday, 28 November 2017, 20:00 +0200 from Sanjay Parab <sparab@linkedin.com>:

SHREATEH **<@gmail.com>**

Dec 11 (4 days ago)

to Sanjay

Dear Sanjay,

Regarding to your last email, Please check the attached file which contains a screenshot that shows linkedin (logged of user)
and the www-authenticate box om Firefox Quantum 57.0.1 (64-bit) (latest Version)

also here is the direct post link depends on your request:
https://www.linkedin.com/feed/update/urn:li:activity:6345943587339014144/

Many thanks.

Attachments area

Sanjay Parab

Dec 11 (4 days ago)

to me

Hi khalil,

Thank you for sharing additional information. We will investigate it and get a response back to you when we have completed our analysis.

Regards,
Sanjay

From: SHREATEH <@gmail.com>
Date: Monday, December 11, 2017 at 3:25 AM
To: Sanjay Parab <sparab@linkedin.com>
Subject: Re: Re[2]: LinkedIn Vulnerability Report

Sanjay Parab Dec 11 (4 days ago)

to me

Hi Khalil,

Thanks for sending additional information. As this requires user interaction, we believe this does not represent security vulnerability.

If you believe there is another way which does not requires user interaction, please write to us.

Regards,
Sanjay

From: Sanjay Parab <sparab@linkedin.com>
Date: Monday, December 11, 2017 at 9:24 AM
To: SHREATEH <@gmail.com>

SHREATEH <@gmail.com> Dec 12 (3 days ago)

to Sanjay

hi sanjay,

this might be the last email from my side, please confirm that this video is not represent a security vulnerability on Linkedin platform : https://youtu.be/EgIJ3WvWMhk

thanks

Attachments area

Preview YouTube video LinkedIn Exploit on Quantum

Sanjay Parab

Dec 13 (2 days ago)

to me

Hi Khalil,

Thank you again for your report and for helping to protect LinkedIn members.
We have taken another look at your report and have confirmed the issue. We are working towards a fix and ask that you not disclose until the fix is in place.
We will be in touch as soon as we have any updates.

Regards,
Sanjay

From: SHREATEH <@gmail.com>
Date: Monday, December 11, 2017 at 10:57 PM
To: Sanjay Parab <sparab@linkedin.com>

SHREATEH <@gmail.com> Dec 13 (2 days ago)

to Sanjay

Good news, surely there won't be any disclose while it still unpatched..

Sanjay Parab 1:28 AM (16 hours ago)

to me

Hi Khalil,

We have confirmed that this issue has now been resolved. Please test it at your end and let us know if your results vary.

We appreciate your efforts to notify us about this issue and want to thank you for helping us to protect LinkedIn members

Regards,
Sanjay

From: SHREATEH <@gmail.com>
Date: Tuesday, December 12, 2017 at 10:18 PM

SHREATEH <@gmail.com> 3:48 PM (2 hours ago)

to Sanjay

Hi Sanjay,

The vulnerability has been patched successfully.

So you guys dont give bounty for security researchers?

kindly, let me know if any further info needed from my side.

BR

SHREATEH <@gmail.com>

5:36 PM (16 minutes ago)

to Tom

--
Regards
khalil-shreateh.com
3 Attachments

Click here to Reply or Forward

2.75 GB (18%) of 15 GB used
Manage

Terms - Privacy

Last account act