

Forum:[Hack Forums](#)

Thread: [Discord Connecting and Account Security](#)

Omniscient - July 28, 2019, 2:25 pm

I have removed the Discord social login. Anyone who had their HF accounts connected to Discord needed to create a full HF account else they've just lost access at least for now. The plugin we used has an exploit of some sort allowing access to the accounts without providing credentials. I am still trying to Reverse Engineer the exploit so we can patch it but felt it was best that until we do the Discord login is removed. Twitter, Facebook, and Google are still available options which at this time I do not believe share the exploit. It seems restricted to just Discord. I suspect it has to do with Discord bots or possibly Discord's API methods. But something is exposed and members were at risk.

Sorry to those that this inconveniences. If you joined HF under our Discord username and never created your own Password then you might be locked out completely. I'm unsure if once we resolve this the account will link again but assume it will not.

This exploit was already used by a scammer but luckily it doesn't appear it was successful and I've spent time on this all week trying to track down how exactly the scammer got ahold of the accounts. Now I know it was our social login plugin and Discord. I'll eventually get the exact method which we'll patch.

Sorry for the inconvenience and thank you.

cobaltstrike - July 28, 2019, 2:26 pm

what if it was just password re-use and the account associated had their emails on dehashed or another leaked db

Omniscient - July 28, 2019, 2:32 pm

(Jul 28, 2019 02:26 PM)cobaltstrike Wrote: [\[CITE\]](#) what if it was just password re-use and the account associated had their emails on dehashed or another leaked db
And yet that's not it.

Careless - July 28, 2019, 2:37 pm

Happy you stopped it in its tracks brilliant work on this.

M L T - July 28, 2019, 3:02 pm

Were you using OAuth by any chance? For discord login integration?

Omniscient - July 28, 2019, 3:09 pm

(Jul 28, 2019 03:02 PM)M L T Wrote: [\[CITE\]](#) Were you using OAuth by any chance? For discord login integration? You know something you want to tell me?

We used a plug-in with some custom alterations for our needs but we really didn't touch the libraries the author used. I am still looking into the code but since it's disabled now it's now #1 priority. Took me a lot of time just to track it down. I have a few other things going on right now which requires my attention.

Tomorrow I will have xerotic take a peek at it. I also offered the scammer see money for exact

details as a bounty. We will find it with or without him though now that I know the entry point.

Discord sucks. This is just more proof of that. Only about 15% of the social connects were discord anyways.

Ram - July 28, 2019, 3:17 pm

Isnt discord prohibited from HF anyways?

duplex - July 28, 2019, 3:20 pm

(Jul 28, 2019 03:17 PM)Ram Wrote: [\[CITE\]](#) Isnt discord prohibited from HF anyways?
Not really

GnosticPlayers - July 28, 2019, 3:22 pm

Thanks Omni. Good move removing the feature entirely :)

Crypto - July 28, 2019, 3:22 pm

(Jul 28, 2019 03:17 PM)Ram Wrote: [\[CITE\]](#) Isnt discord prohibited from HF anyways?
I guess not anymore, I wasn't very active for some weeks but when I came "back" I saw people suddenly posting their discord information like it wasn't prohibited anymore...

Anyways thanks Omni for keeping our accounts safe & being on top of it once again when the site's security is at risk.

Your dedication is inspiring for sure.

Meow - July 28, 2019, 3:24 pm

(Jul 28, 2019 03:17 PM)Ram Wrote: [\[CITE\]](#) Isnt discord prohibited from HF anyways?I believe you're not allowed to link to a Discord server but you're allowed to advertise your Discord username (same with Skype/Telegram).

Crypto - July 28, 2019, 3:29 pm

(Jul 28, 2019 03:24 PM)Meow Wrote: [\[CITE\]](#) I believe you're not allowed to link to a Discord server but you're allowed to advertise your Discord username (same with Skype/Telegram).

Your right.

M L T - July 28, 2019, 3:51 pm

(Jul 28, 2019 03:09 PM)Omniscient Wrote: [\[CITE\]](#) You know something you want to tell me?

We used a plug-in with some custom alterations for our needs but we really didn't touch the libraries the author used. I am still looking into the code but since it's disabled now it's now #1 priority. Took me a lot of time just to track it down. I have a few other things going on right now which requires my attention.

Tomorrow I will have xerotic take a peek at it. I also offered the scammer see money for exact details as a bounty. We will find it with or without him though now that I know the entry point.

Discord sucks. This is just more proof of that. Only about 15% of the social connects were discord anyways.

No specific reason I'm asking, I was just curious because it's possible to hijack sessions via OAuth integration if it's misconfig'd + if someone managed to find an open redirect on *.hackforums.net somewhere (which I believe exist within the tracking subdomain) - I was just curious if someone

maybe pulled an attack similar to [what I'm describing here](#) -- the same concept could apply for any OAuth linked application although I'm using facebook in my description. I was just figuring someone maybe abused OAuth integration paired with an open redirect in one of your domains to hijack user accounts, and maybe that could have been the issue.

Just a guess is all, I've no idea what went down nor have I heard anything.. If you were using OAuth though, depending upon how it's configured, someone could have used it to hijack accounts by pairing it with one of the open redirects in your 'tracking' subdomain. I'm unsure if you've found the root cause, and maybe I'm totally in the wrong ball park here, but if you were using OAuth maybe it's worth looking into that as the possible source of the problem.

EDIT: [this report](#) explains what I'm talking about fairly well... like I said though, no idea if the issue you're having is related to OAuth, just speculation.

Sigma - July 28, 2019, 4:46 pm

(Jul 28, 2019 03:51 PM)M L T Wrote: [\[CITE\]](#) No specific reason I'm asking, I was just curious because it's possible to hijack sessions via OAuth integration if it's misconfig'd + if someone managed to find an open redirect on *.hackforums.net somewhere (which I believe exist within the tracking subdomain) - I was just curious if someone maybe pulled an attack similar to [what I'm describing here](#) -- the same concept could apply for any OAuth linked application although I'm using facebook in my description. I was just figuring someone maybe abused OAuth integration paired with an open redirect in one of your domains to hijack user accounts, and maybe that could have been the issue.

Just a guess is all, I've no idea what went down nor have I heard anything.. If you were using OAuth though, depending upon how it's configured, someone could have used it to hijack accounts by pairing it with one of the open redirects in your 'tracking' subdomain. I'm unsure if you've found the root cause, and maybe I'm totally in the wrong ball park here, but if you were using OAuth maybe it's worth looking into that as the possible source of the problem.

EDIT: [this report](#) explains what I'm talking about fairly well... like I said though, no idea if the issue you're having is related to OAuth, just speculation.

I have seen this report too. I am glad it is getting removed, too risky.

JustMadeAnotherAltAcc0unt - July 28, 2019, 4:49 pm

How am i a scammer? i just want my data removed like i already asked on discord :). kindly do it please

GnosticPlayers - July 28, 2019, 4:53 pm

(Jul 28, 2019 04:49 PM)JustMadeAnotherAltAcc0unt Wrote: [\[CITE\]](#) How am i a scammer? i just want my data removed like i already asked on discord :). kindly do it pleaseYou're wasting your time, bud. You shouldn't care about anything online if you're smart.

Ram - July 29, 2019, 2:08 am

(Jul 28, 2019 03:29 PM)Crypto Wrote: [\[CITE\]](#)

Your right.

That apparently changed cuz I posted my username in my sales thread few months back and got 50% warning.

flavoral - July 29, 2019, 8:14 am

(Jul 29, 2019 02:08 AM)Ram Wrote: [\[CITE\]](#) That apparently changed cuz I posted my username in my sales thread few months back and got 50% warning.

Yeah the rule changed few weeks ago.

Ram - July 29, 2019, 8:49 am

(Jul 29, 2019 08:14 AM)flavoral Wrote: [\[CITE\]](#) Yeah the rule changed few weeks ago.

That rule didnt make sense anyways so im glad its changed cuz its essentially the same shit as skype lol

flavoral - July 29, 2019, 9:34 am

(Jul 29, 2019 08:49 AM)Ram Wrote: [\[CITE\]](#) That rule didnt make sense anyways so im glad its changed cuz its essentially the same shit as skype lol

it did due to imposters and being using special characters with carded nitro to look legit and scam.

duck - July 29, 2019, 9:52 am

Fuck discord!!!!!!

Shit application

M L T - July 29, 2019, 10:02 am

(Jul 29, 2019 09:52 AM)duck Wrote: [\[CITE\]](#) fugg discord!!!!!!

Shit application

Agreed. The fact you can remotely infect anyone who has the client installed without any warning or prompt just as a result of them visiting your webpage should be proof enough that discord is a heap of shit.

In fact, people should just stop using Electron Framework in general. It's riddled w/ vulnerabilities. I'm laughing at the fact the infosec community are only now just starting to discover discord/electron bugs that we've been sitting on for 2.5yrs+

The only thing that's more of a joke than Discord itself, is Discord's "bug bounty program" -- they paid me \$150 for shell access to discordapp.com, I could have literally auto-updated everyone's client with a backdoor if I felt like it. Also, they claimed that they pay out \$100 for crash methods, so I reported 15+ methods of crashing the client and got ignored. I reported the discord:// and file:// uri argument injection vulns years back and they're only just now getting around to patching them.

Watching Discord devs attempt to patch vulns is like watching the special olympics. They "fixed" the file:// uri + webdav 0day by making it so that you couldn't use in-client "tagging" to make custom URI schemes clickable... bypass? Just load the file:// uri into an iframe src and link someone to your website instead... if anything it's more stealthy, and bypassed their patch entirely. Honestly I swear the entire discord development team have less brain cells than employees.

duck - July 29, 2019, 10:05 am

(Jul 29, 2019 10:02 AM)M L T Wrote: [\[CITE\]](#) Agreed. The fact you can remotely infect anyone who has the client installed without any warning or prompt just as a result of them visiting your webpage should be proof enough that discord is a heap of shit.

In fact, people should just stop using Electron Framework in general. It's riddled w/ vulnerabilities. I'm laughing at the fact the infosec community are only now just starting to discover discord/electron bugs that we've been sitting on for 2.5yrs+

The only thing that's more of a joke than Discord itself, is Discord's "bug bounty program" -- they paid me \$150 for shell access to discordapp.com, I could have literally auto-updated everyone's client with a backdoor if I felt like it. Also, they claimed that they pay out \$100 for crash methods, so I reported 15+ methods of crashing the client and got ignored. I reported the discord:// and file:// uri argument injection vulns years back and they're only just now getting around to patching them.

Watching Discord devs attempt to patch vulns is like watching the special olympics. They "fixed" the

file:// uri + webdav Oday by making it so that you couldn't use in-client "tagging" to make custom URI schemes clickable... bypass? Just load the file:// uri into an iframe src and link someone to your website instead... if anything it's more stealthy, and bypassed their patch entirely. Honestly I swear the entire discord development team have less brain cells than employees.

Discord is a extreme data-mining application.

I wouldn't be expected seeing some case like with facebook last year but with discord.

Discord is extremely in-secure application, and in terms of privacy I rather not even mention word. Discord is joke, they make it look how cool we are but in reality they are group of pedos that spies on kids.

I rather not talk about discord as it makes me very mad hearing that word. DISCORD oh my goshhhhhh

M L T - July 29, 2019, 10:26 am

(Jul 29, 2019 10:05 AM)duck Wrote: [\[CITE\]](#) Discord is a extreme data-mining application.

I wouldn't be expected seeing some case like with facebook last year but with discord.

Discord is extremely in-secure application, and in terms of privacy I rather not even mention word. Discord is joke, they make it look how cool we are but in reality they are group of pedos that spies on kids.

I rather not talk about discord as it makes me very mad hearing that word. DISCORD oh my goshhhhhh

have you actually ever read their privacy policy / terms of service? its batshit insane, basically states "ANYTHING YOU TYPE, POST, OR SAY, IS OUR INTELLECTUAL PROPERTY" -- of course that's para-phrasing, but that's literally what their privacy policy and ToS alludes to.

Omniscient - July 29, 2019, 10:28 am

Quote:That rule didnt make sense anyways so im glad its changed cuz its essentially the same shit as skype lol

Discord is no way the same as Skype.

Discord is the worst shit on the planet right now.

Quote:The only thing that's more of a joke than Discord itself, is Discord's "bug bounty program" -- they paid me \$150 for shell access to discordapp.com, I could have literally auto-updated everyone's client with a backdoor if I felt like it. Also, they claimed that they pay out \$100 for crash methods, so I reported 15+ methods of crashing the client and got ignored. I reported the discord:// and file:// uri argument injection vulns years back and they're only just now getting around to patching them.

You should have just put that shit into the wild.

duck - July 29, 2019, 10:30 am

(Jul 29, 2019 10:26 AM)M L T Wrote: [\[CITE\]](#) have you actually ever read their privacy policy / terms of service? its batshit insane, basically states "ANYTHING YOU TYPE, POST, OR SAY, IS OUR INTELLECTUAL PROPERTY" -- of course that's para-phrasing, but that's literally what their privacy policy and ToS alludes to.

i read it not only once.

its crazy what they say i remember their privacy policy contained something like that they can share your personal information with anyone but especially is shared with all technicians working for discord.

discord is nightmare, they store every information about you and also making offline backups i

believe.

btw Discord seems to be hosted on Google servers, so big no.

fuck discord never want to hear this word again.

omniscient should make filter for discord to shitcord or something like that.

it's evilness!!!

(Jul 29, 2019 10:28 AM)Omniscient Wrote: [\[CITE\]](#) Discord is the worst shit on the planet right now.

please make a censure for discord.

i hate seeing this word.

kind regards our lord omniscient ?

M L T - July 29, 2019, 10:38 am

(Jul 29, 2019 10:28 AM)Omniscient Wrote: [\[CITE\]](#) You should have just put that shit into the wild.

We put some other discord/electron bugs into the wild. Right now it's still possible to RCE users, you can silently infect them with malware just as a result of them clicking a URL... pretty crazy. To be fair though, it's an electron-specific bug, meaning Slack, Skype for Windows, Github Desktop, some torrent clients, a few bitcoin clients and more are also affected... but, all of these other applications, when the URI scheme is launched, it pops up with a message asking which application you'd like to use to open the link. Discord though? No message at all... just silently runs that shit in the background :|

This method right here (very similar to what I just described) also has a current working bypass for its patch:

[Video: <https://www.youtube.com/watch?v=yWzVeS5hC8A>]

See how it executes the file in addition to downloading it? Crazy.. discord devs certainly have their heads stuck up their asses.

Btw, was I right in guessing the Discord issue was OAuth related, or was it something else entirely? Just curious is all.

Cooligan - July 29, 2019, 11:51 am

(Jul 28, 2019 03:17 PM)Ram Wrote: [\[CITE\]](#) Isn't discord prohibited from HF anyways?

(Jul 28, 2019 03:22 PM)Crypto Wrote: [\[CITE\]](#) I guess not anymore, I wasn't very active for some weeks but when I came "back" I saw people suddenly posting their discord information like it wasn't prohibited anymore...

Anyways thanks Omni for keeping our accounts safe & being on top of it once again when the site's security is at risk.

Your dedication is inspiring for sure.

(Jul 29, 2019 02:08 AM)Ram Wrote: [\[CITE\]](#) That apparently changed cuz I posted my username in my sales thread few months back and got 50% warning.

All of this.

You're now able to link your discord as a contact option, however you're still unable to link any discord servers.