

Forum:[Hack Forums](#)

Thread: [Hack Target By Discord Name - Tutorial - No SE](#)

AU Subi - April 12, 2018, 6:05 pm

Today I will be disclosing a Oday exploit, which involves sending a crafted payload to a target's Discord client, which will result in remote code execution, and ultimately, download and execute your malware. This attack involves creating a malformed Discord server, and sending an invitation to your victim. It merely requires permissions to send messages to the victim.

Creating the Server

When we create a server on Discord, there are a few arguments the server-creation function must first take in order to create your server. For this exploit, we will modify restricted arguments using a binary-dithering attack on the Discord central server node heap. First, we will take a look at the packet involved in creating a Discord server:

```
5E 01 9E 01 4E 11 00 01 01 00 01 00
```

The structure of this packet should be self-explanatory. The value of interest is the last boolean, which can be set to 1 in order to extend the packet structure and provide further arguments. Structure of extended packet:

```
[old_packet] 5E 98 41 00 FE 26 AC 7E
```

Our goal is to modify this vectored session handler to reduce entropy and create arbitrary runtime noise disturbances, which will create an ample time window for certain race conditions. In order to do this, we must modify the MSB (most significant byte) in order to create an unfolding bit collapse situation. The issue is, this vectored session handler is encrypted with AES-192 initialized by a buffered XMS binary tree, which is left-leaning and contains multiple node indexing caches. No need to worry about the complex encryption, though, as we can simply bruteforce it, as there are only BYTE_MAX (256) different possible combinations. The server's response is encrypted, so knowing when the bruteforce attack is successful was a problem, but I discovered the response simply differs in length from the fail response, it is 9 bytes long whereas the fail response is 7.

Once you have received the success response you will need to quickly inject another command, as you have created an ample time window with this previous payload in order to perform a race condition. The race condition we are performing will overwrite dynamic heap objects and ring0 paged memory SSDTs, corrupting the call-stack and allowing us to overwrite Discord server object data with arbitrary shellcode. The shellcode we write will contain the code we want to execute, and some NOP sleds in order to return propagated constants and security seeds to their original values. The command we will execute to trigger this race condition is an unused Discord user API feature pulled from the client code, the packet is:

```
FF FF 05 00 00 00
```

You will need to inject this within a 7-10 ms time window, otherwise the race condition will miss. Do it earlier than 7 ms, it will fail, do it later than 10, it will fail. You can increase this time window by buffing up your Discord user data to a considerable size. To know whether it has succeeded or failed, simply send your shellcode up the TCP stream at any time and then send the server create command. If successful, you should have a malformed Discord server. Simply send an invitation to

your target via right-click~>invite to server and the payload will execute as soon as the invitation is received.

I won't spoonfeed the shellcode but I'll give away the necessities, you need a 12 byte nop sled at the beginning, and 3 five byte ones at index 18, 82, and 111. The rest of the shellcode is up to you, hint: download and execute. This is how a malformed server invitation should look:

Happy exploiting.

Slim Jxmmi - April 12, 2018, 6:12 pm

This doesn't work for anyone who's wondering.

SysAdmin - April 12, 2018, 6:14 pm

(Apr 12, 2018 06:12 PM)Slim Jxmmi Wrote: [\[CITE\]](#) This doesn't work for anyone who's wondering. But he's Master Hacker!?!?!?

Slim Jxmmi - April 12, 2018, 6:15 pm

(Apr 12, 2018 06:14 PM)SysAdmin Wrote: [\[CITE\]](#) But he's Master Hacker!?!?!?
Oh... shit! My fucking bad.

Nevermind guys! This guy is a Master Hacker who may also have a 0day in HF.

GlobalLine - April 12, 2018, 6:16 pm

(Apr 12, 2018 06:12 PM)Slim Jxmmi Wrote: [\[CITE\]](#) This doesn't work for anyone who's wondering. This especially won't work if they're using the browser version.

SupremeLV - April 12, 2018, 6:16 pm

(Apr 12, 2018 06:14 PM)SysAdmin Wrote: [\[CITE\]](#) But he's Master Hacker!?!?!?
Fuck :(I was looking forward to his 1337 hacker skills :(

Slim Jxmmi - April 12, 2018, 6:16 pm

(Apr 12, 2018 06:16 PM)GlobalLine Wrote: [\[CITE\]](#) This especially won't work if they're using the browser version.
It wouldn't work on any version.

AU Subi - April 12, 2018, 6:27 pm

(Apr 12, 2018 06:12 PM)Slim Jxmmi Wrote: [\[CITE\]](#) This doesn't work for anyone who's wondering. This works, stop trying to gate-keep and prevent this exploit from being used widespread. Thanks.

(Apr 12, 2018 06:16 PM)GlobalLine Wrote: [\[CITE\]](#) This especially won't work if they're using the browser version.

Correct, this exploit does not work for the browser version.

BlazinBlunts - April 12, 2018, 6:36 pm

This kid is a fucking idiot lol

??t? - April 12, 2018, 7:08 pm

Does this work on facebook

I need to know if my gf is cheating on me

AU Subi - April 12, 2018, 7:44 pm

(Apr 12, 2018 07:08 PM)???t? Wrote: [\[CITE\]](#) Does this work on facebook
I need to know if my gf is cheating on me
This reply deserves an award lol

BlazinBlunts - April 13, 2018, 2:27 pm

(Apr 12, 2018 07:44 PM)AU Subi Wrote: [\[CITE\]](#) This reply deserves an award lol
For what reason? A lot of people come here for that reason. You really are autistic lmao

AU Subi - April 13, 2018, 2:36 pm

(Apr 13, 2018 02:27 PM)Cryptobro Wrote: [\[CITE\]](#) For what reason? A lot of people come here for that reason. You really are autistic lmao
You have been following me around on 3 threads now. I know you are in love with me but please tone it down, thanks

cameltoejoe - April 13, 2018, 9:54 pm

(Apr 12, 2018 07:08 PM)???t? Wrote: [\[CITE\]](#) Does this work on facebook
I need to know if my gf is cheating on me
I'll pray for you tonight my friend..... ?