

Forum:[Hack Forums](#)

Thread: [Chain of Exploit to Gain Access as Root User In Android](#)

GolemX - April 23, 2018, 1:36 pm

I want to build chain exploit to gain access as root user in Android. I wanted exploit to work perfectly below Android 6(Lollipop). To Build this we need at least I think 3 vulnerability. The first vulnerability is a V8 engine type confusion bug which can be utilised for remote code execution in sandboxed Chrome render process environments.

[Click Here to know more about this vulnerability](#)

The second security flaw is found in Android's libgralloc module and can be used to escape from Chrome's sandbox due to a map and unmap mismatch, which can, in turn, prompt a Use-After-Unmap error.

Dirty Cow vulnerability can be used to gain access on Android system. I want to combine all these exploit and build a new exploit. This new exploit should work when a URL in Chrome is accessed. I want payload to be executed in android system as root user.

The whole point is to gain access as root shell(user) in android through URL in chrome. Hope you got picture of what I am trying to explain.

[Click Here to Know More About Dirty Cow Exploit](#)

So anybody could help me in this, I will give reward also to person who help me achieve this Goal