One day short...

Consists of three major exploits, CVE-2020-15972, CVE-2020-16045, CVE-2020-11239. These create a full exploit chain where malicious code can be run on the chrome browser, achieve RCE in chrome, escape the chrome jail, then achieve kernel code execution

Malicious code run from website

CVE-2020-15972

Exploit on the chrome renderer to achieve RCE within the chrome sandbox. This will enable the execution of another exploit that will allow the program to escape the chrome sandbox and start running code in android userland.

RCE achieved on chrome sandbox

CVE-2020-16045

Exploit in the chrome sandbox allowing an escape to android userland with. Requires RCE on the chrome sandbox before being applicable.

RCE on android userland

CVE-2020-11239

Use after free exploit in the Qualcomm Kernel Graphics support layer allowing a user to achieve arbitrary code execution. The user achieves arbitrary read and write using a fulnerability in the Qualcomm KGSL, then uses the arbitrary memory write to execute their written memory in kerneland using a `__bpf_prog_run32 function call.`

Privilege escalation achieved

Project Zero

Consists of five main exploits, CVE-2022-4262, CVE-2022-3038, CVE-2022-22706, CVE-2023-0266, and CVE-2023-26083. The first two deal with chrom exploits. The remaining deal with achieving privilege escalation in the andriod kernel.

Malicious code run from website

CVE-2022-4262

Exploit using type confusion in chrome to achieve rce via heap corruption within the chrome sandbox. This will enable execution of exploit CVE-2022-3038 to escape the chrome sandbox.

RCE achieved on chrome sandbox

CVE-2022-3038

UAF in crhome sandbox allowing an escape to andoid userland.

RCE on android userland

CVE-2022-22706

An exploit in the mali gpu kernele driver allowing for arbitrary write access to read only memory pages for non-privileged users. This is used to achieve full userland code write and execution privileges.

execution as system_server achieved

CVE-2023-0266

race condition in the 32-bit compatability layer of the ALSA driver allows a user to free an object containing user controlled data and reclaim it with a powerful heap-spray technique usinng highly detailed and controlled struct snd_kcontrol objects.

CVE-2023-26083

Mali gpu driver exploit allows users to access kernel pointers to objects within the kernel and write 16 byters into known kernel addresses. Using this in tandem with CVE-2023-0266, an attacker is able to fill struct snd_kcontrol objects with pointers to the attacker controlled data created using CVE-2023-0266 and achieve privlege escalation.

Privilege escalation achieved.