

PACER: Threat Intelligence Report (TIR)

INDEX

SECTION A. DEVICE INFORMATION..... PAGE NO=2

A1. APPLICATIONS INSTALLED ON THE DEVICE..... PAGE NO=2

A2. SERVICES RUNNING ON THE DEVICE..... PAGE NO=5

A3. THIRD PARTY APPLICATIONS..... PAGE NO=6

SECTION B. MALWARE REPORT..... PAGE NO=7

B1. MALWARE REPORT OF THE DEVICEPAGE NO=7

SECTION C. CVE REPORT..... PAGE NO=10

C1. CVE REPORT OF THE DEVICE..... PAGE NO=10

SECTION D. SUGGESTIONS..... PAGE NO=

D1. SUGGESTION FOR UPDATION OF APPS.....PAGE NO=16

D2. SUGGESTION FOR DELETION OF APPS ... PAGE NO=17

PACER: Threat Intelligence Report (TIR)

Section A. DEVICE INFORMATION

Information Of Device

Date: 08-01-20

Device Name: VIVO (AMKZ7LUOCQLR95JB)

Product: 1601

Model number: vivo_1713

Device: 1601

transport_id: 1

RAM: Total Space= 4.00GB

Storage Capacity: Total Space= 64GB; Available Space= 17.34GB

IMEI 1: 866054034440677

IMEI 2: 866054034440669

Android version: 7.0

Android Security Patch level: 2019-06-05

Processor: 1.5GHz Octa-core

vivo ROM : Funtouch OS_3.2

Software version : PD1612DF_EX_A_3.14.2

Baseband version: MOLY.LR11.W1603.MD.MP.V44.P111, 2019/04/09 15:41

Kernel version : 3.18.35

Compile time: 2019-06-21

Applications Installed

Number of Applications installed on Device: 303

Applications installed on the Device-Vivo

com.mediatek.gba	com.bbk.iqoo.logsystem
com.mediatek.ims	com.cootek.smartinputv5.language.oem.tagalog
com.google.android.apps.subscriptions.red	com.vivo.SmartKey
com.android.cts.priv.ctsshim	com.google.android.apps.docs
com.nestik.kalilinux	com.google.android.apps.maps
com.gd.mobicore.pa	com.microsoft.office.word
com.google.android.youtube	com.cootek.smartinputv5.language.oem.hindilatin
org.simalliance.openmobileapi.uicc2terminal	com.bbk.facewake
com.bbk.logservice	com.google.android.webview
com.google.android.ext.services	com.microsoft.office.powerpoint
com.android.providers.telephony	com.cootek.smartinputv5.language.oem.indiansanskrit
com.vivo.smartmultiwindow	com.cootek.smartinputv5.language.oem.indiansanthali
com.vivo.fuelssummary	com.android.server.telecom
com.truecaller	com.google.android.syncadapters.contacts
com.google.android.googlequicksearchbox	com.vivo.permissionmanager
com.android.providers.calendar	com.android.keychain
com.indiainfoline	com.cootek.smartinputv5.language.oem.chs
com.android.providers.media	com.cootek.smartinputv5.language.oem.cht
com.cootek.smartinputv5.language.oem.indiansindhi	com.android.camera
com.vivo.livewallpaper.coffeetime	com.android.chrome
com.cootek.smartinputv5.language.oem.malayan	ai.wizely.android
com.cootek.smartinputv5.language.oem.marathi	com.bbk.launcher2

com.nextbillion.groww
com.vivo.setupwizard
com.google.android.onetimeinitializer
com.mediatek.fwk.plugin
com.google.android.ext.shared
com.vivo.easysshare
com.cootek.smartinputv5.skin.keyboard_vivo
com.cootek.smartinputv5.language.oem.indianmaithili
com.vivo.abe
com.vivo.pem
com.android.wallpapercropper
com.mediatek.schpwronoff
com.sp.protector.free
com.sololearn
com.vivo.safecenter
com.vivo.appfilter
com.cootek.smartinputv5.language.oem.indianmanipuri
com.vivo.collage
com.vivo.compass
org.simalliance.openmobileapi.service
com.myairtelapp
com.vivo.mediatune
com.android.documentsui
com.android.externalstorage
com.mediatek.ygps
com.paprbit.dcoder
com.android.htmlviewer
com.whatsapp
com.vivo.cameraparamluma
com.android.DemoVideo
com.android.mms.service
com.google.android.apps.docs.editors.sheets
com.cootek.smartinputv5.language.oem.thai
com.cootek.smartinputv5.language.oem.urdu
com.android.providers.downloads
com.mediatek.engineermode
com.android.bbkmusic
com.mediatek.omacp
com.bbk.ftplog
com.android.browser
com.bbk.updater
com.android.bbkcalculator
com.google.android.configupdater
com.cootek.smartinputv5.language.oem.russian
com.cootek.smartinputv5.language.oem.indiankonkani
com.vivo.ewarranty
com.vivo.pushservice
com.mediatek.wfo.impl
com.volte.config
com.android.defcontainer
com.android.vending
com.android.pacprocessor
com.cootek.smartinputv5.language.oem.indiandogri
com.android.filemanager
com.microsoft.skydrive
com.flipkart.android
com.android.certinstaller
com.vivo.smartshot
com.google.android.marvin.talkback
com.cootek.smartinputv5.language.oem.indianbodo
android
com.android.contacts
com.vivo.secime.service
com.emoji.keyboard.touchpal.vivo
com.vivo.upnpserver
com.bitstrips.imoji

com.cootek.smartinputv5.language.oem.hinglish
com.android.dialer
com.google.android.installer
com.google.android.gms
com.google.android.gsf
com.google.android.tts
com.android.callogbackup
com.google.android.partnersetup
com.google.android.videos
com.saavn.android
com.vivo.networkstate
com.vivo.livewallpaper.silk
com.android.proxyhandler
com.cootek.smartinputv5.language.oem.gujarati
com.vivo.widget.calendar
com.vivo.magazine
com.android.VideoPlayer
com.cootek.smartinputv5.language.oem.indonesian
com.android.BBKCrontab
com.android.musiceffecttest
com.zhiliaoapp.musically
com.google.android.feedback
com.google.android.printservice.recommendation
com.google.android.apps.photos
com.google.android.syncadapters.calendar
com.vivo.doubletimezoneclock
com.android.managedprovisioning
com.spotify.music
com.iqoo.secure
com.mediatek.atci.service
com.cootek.smartinputv5.language.oem.kannada
com.mventus.selfcare.activity
com.vivo.sim.contacts
com.udemy.android
com.mediatek.thermalmanager
com.cootek.smartinputv5.language.oem.arabic
com.iqoo.powersaving
com.android.skintwo
com.android.providers.partnerbookmarks
com.google.android.gsf.login
com.mtk.telephony
com.northpark.drinkwater
com.cootek.smartinputv5.language.oem.french
com.cootek.smartinputv5.language.oem.german
com.facebook.system
com.vivo.networkimprove
com.gaana
com.android.bbk.lockscreen3
com.baidu.map.location
com.vivo.audiofx
com.meetup
srl.midnighttea.pushit
com.adobe.reader
com.google.android.backuptransport
com.cootek.smartinputv5.language.oem.nepali
com.cootek.smartinputv5.language.oem.malayalam
com.nike.ntc
com.bbk.theme.resources
com.storybeat
com.android.bookmarkprovider
com.android.settings
com.google.android.apps.nbu.paisa.user
com.cisco.webex.meetings
com.cootek.smartinputv5.language.oem.somali
com.bbk.scene.indoor
com.cootek.smartinputv5.language.oem.telugu

com.sonyliv
com.confirmtkl.lite
com.bbk.cloud
com.cootek.smartinputv5.language.oem.indiankashmiri
com.bbk.theme
com.ryzac.codecademygo
com.microsoft.launcher
com.android.egg
com.android.mms
com.android.mtp
com.android.stk
com.android.backupconfirm
com.instagram.android
com.android.tethersettings
com.mediatek.bluetooth.dtt
com.cootek.smartinputv5.language.oem.sinhala
com.microsoft.office.onenote
com.hp.orbit
com.focaltech.ft_waferedge_test
com.bbk.calendar
com.android.statementservice
com.android.BBKClock
in.startv.hotstar
com.google.android.gm
com.android.BBKTools
org.chromium.webapk.a879f9decdbb68787
com.cootek.smartinputv5.language.oem.santhali
com.android.photoeditor
com.mycaptain.app
com.google.android.apps.tachyon
com.mediatek.mdmlsample
com.android.wifisettings
com.vlife.vivo.wallpaper
com.ionicframework.someapp771914
com.microsoft.emmx
com.vivo.daemonService
com.mediatek.providers.drm
com.cootek.smartinputv5.language.oem.spanish
com.ringclip
com.google.android.instantapps.supervisor
com.olacabs.customer
com.avenuegrowth
com.google.android.setupwizard
com.iqoo.engineermode
com.android.BBKPhoneInstructions
com.android.providers.settings
com.mediatek.miravision.ui
com.android.sharedstoragebackup
com.google.android.music
com.android.printspooler
org.simalliance.openmobileapi.uicc1terminal
com.vivo.dream.note
com.android.incallui
cc.blynk
com.android.inputdevices
com.android.bluetoothsettings
com.bbk.photoframewidget
com.android.vivo.mtklog
com.android.skin
com.mediatek
com.google.android.apps.nbu.files
com.example
com.ibimuyu.lockscreen
com.google.android.apps.classroom

com.nexstreaming.app.kinemasterfree
com.mediatek.lbs.em2.ui
com.android.cts.ctsshim
com.cootek.smartinputv5.language.oem.punjabi
com.cootek.smartinputv5.language.oem.bengali
com.cootek.smartinputv5.language.oem.assamese
com.cootek.smartinputv5.language.oem.zawgyi
com.vivo.dream.clock
com.vivo.dream.music
com.vivo.upslide
com.goibibo
com.android.vpndialogs
com.vivo.gallery
com.cootek.smartinputv5.language.oem.indiankonkanikn
com.vivo.email
com.vivo.flash
com.cootek.smartinputv5.language.oem.laotian
com.vivo.gamewatch
com.android.notes
com.android.phone
com.android.shell
com.vivo.fingerprint
com.cootek.smartinputv5.language.oem.hindi
com.cootek.smartinputv5.language.oem.khmer
com.android.wallpaperbackup
com.cootek.smartinputv5.language.oem.oriya
com.android.providers.blockednumber
com.cootek.smartinputv5.language.oem.tamil
com.android.providers.userdictionary
com.vivo.minscreen
com.intsig.camscanner
com.vivo.FMRadio
com.android.location.fused
com.android.systemui
com.vivo.livewallpaper.coralsea
com.android.bluetoothmidiservice
com.vivo.doubleinstance
com.vivo.appstore
com.facebook.appmanager
com.bbk.SuperPowerSave
com.cootek.smartinputv5.language.oem.burmese
com.vivo.browser
club.fromfactory
com.mediatek.mtklogger
com.focaltech.ft_terminal_test
com.vivo.bsptest
com.vivo.motionrecognition
com.android.skinfive
com.mediatek.sensorhub.ui
com.cootek.smartinputv5.language.oem.manipuri
in.gov.swayam.app
com.android.bluetooth
com.android.providers.contacts
no.mobitroll.kahoot.android
com.android.captiveportallogin
com.cootek.smartinputv5.language.oem.vietnam
com.android.skinthree
cn.wps.moffice_eng
com.snapchat.android
com.android.bbksoundrecorder
com.cootek.smartinputv5.language.oem.cangjie
com.bbk.account

Services Running On The Device

Number of services running on Device: **149** services

List of Services Running On the Device-Vivo

0	gamewatch_server: [com.vivo.gamewatch.common.IGameWatch]	75	network_management: [android.os.INetworkManagementService]
1	GbaService: [com.mediatek.gba.IGbaService]	76	clipboard: [android.content.IClipboard]
2	GpuAppSpectatorService: [com.mediatek.GpuAppSpectatorService]	77	statusbar: [com.android.internal.statusbar.IStatusBarService]
3	carrier_config: [com.android.internal.telephony.ICarrierConfigLoader]	78	device_policy: [android.app.admin.IDevicePolicyManager]
4	phoneEx: [com.mediatek.internal.telephony.ITelephonyEx]	79	deviceidle: [android.os.IDeviceIdleController]
5	phone: [com.android.internal.telephony.ITelephony]	80	persistent_data_block: [android.service.persistentdata.IPersistentDataBlockService]
6	isms: [com.android.internal.telephony.ISms]	81	lock_settings: [com.android.internal.widget.ILockSettings]
7	iphonesubinfo: [com.android.internal.telephony.IPhoneSubInfo]	82	uimode: [android.app.IUiModeManager]
8	simphonebook: [com.android.internal.telephony.IIccPhoneBook]	83	mount: [IMountService]
9	isub: [com.android.internal.telephony.ISub]	84	accessibility: [android.view.accessibility.IAccessibilityManager]
10	ims: [com.android.ims.internal.IImsService]	85	input_method: [com.android.internal.view.IInputMethodManager]
11	telecom: [com.android.internal.telecom.ITelecomService]	86	input_method_secure: [com.android.internal.view.IInputMethodManager]
12	wfo: [com.mediatek.wfo.IWifiOffloadService]	87	pinner: []
13	contexthub_service: [android.hardware.location.IContextHubService]	88	vrmanager: [android.service.vr.IVrManager]
14	dns_listener: [android.net.metrics.IDnsEventListener]	89	input: [android.hardware.input.IInputManager]
15	connectivity_metrics_logger: [android.net.IConnectivityMetricsLogger]	90	window: [android.view.IWindowManager]
16	bluetooth_manager: [android.bluetooth.IBluetoothManager]	91	alarm: [android.app.IAlarmManager]
17	imms: [com.android.internal.telephony.IMms]	92	consumer_ir: [android.hardware.IConsumerIrService]
18	media_projection: [android.media.projection.IMediaProjectionManager]	93	vibrator: [android.os.IVibratorService]
19	mtk-perfservice: [com.mediatek.perfservice.IPerfService]	94	content: [android.content.IContentService]
20	launcherapps: [android.content.pm.ILauncherApps]	95	account: [android.accounts.IAccountManager]
21	shortcut: [android.content.pm.IShortcutService]	96	media.camera.proxy: [android.hardware.ICameraServiceProxy]
22	fingerprint: [android.hardware.fingerprint.IFingerprintService]	97	telephony.registry: [com.android.internal.telephony.ITelephonyRegistry]
23	trust: [android.app.trust.ITrustManager]	98	scheduling_policy: [android.os.ISchedulingPolicyService]
24	media_router: [android.media.IMediaRouterService]	99	webviewupdate: [android.webkit.IWebViewUpdateService]
25	media_session: [android.media.session.ISessionManager]	100	usagstats: [android.app.usage.IUsageStatsManager]
26	restrictions: [android.content.IRestrictionsManager]	101	battery: []
27	print: [android.print.IPrintManager]	102	sensorservice: [android.gui.SensorServer]
28	graphicsstats: [android.view.IGraphicsStats]	103	anrmanager: [android.app.IANRManager]
29	assetatlas: [android.view.IAssetAtlas]	104	processinfo: [android.os.IProcessInfoService]
30	dreams: [android.service.dreams.IDreamManager]	105	permission: [android.os.IPermissionController]
31	sar_power_service: [com.vivo.services.sarpower.ISarPowerStateService]	106	cpuinfo: []
32	vivo_perf_service: [com.vivo.services.perfservice.IVivoPerfService]	107	dbinfo: []
33	motion_manager: [com.vivo.services.motion.IMotionManager]	108	gfxinfo: []
34	hall_state_service: [com.vivo.services.hallstate.IHallManager]	109	meminfo: []
35	vivo_prox_cali_service: [com.vivo.services.proxcali.IVivoProxCaliService]	110	procstats: [com.android.internal.app.procstats.IProcessStats]
36	engineer_utilite: [com.vivo.services.engineerutile.IBBKEngineerUtileService]	111	activity: [android.app.IActivityManager]
37	bbk_touch_screen_service: [com.vivo.services.touchscreen.IBBKTouchScreenService]	112	user: [android.os.IUserManager]
38	commontime_management: []	113	otadexopt: [android.content.pm.IOtaDexopt]
39	network_time_update_service: []	114	package: [android.content.pm.IPackageManager]
40	samplingprofiler: []	115	display: [android.hardware.display.IDisplayManager]
41	diskstats: []	116	power: [android.os.IPowerManager]
42	voiceinteraction: [com.android.internal.app.IVoiceInteractionManagerService]	117	appops: [com.android.internal.app.IAppOpsService]
43	appwidget: [com.android.internal.appwidget.IAppWidgetService]	118	batterystats: [com.android.internal.app.IBatteryStats]
44	backup: [android.app.backup.IBackupManager]	119	rms: [com.vivo.rms.IRM]
45	soundtrigger: [com.android.internal.app.ISoundTriggerService]	120	netd: []
46	jobscheduler: [android.app.job.IJobScheduler]	121	media.mmsdk: [com.mediatek.mmsdk.IMMSdkService]
47	hardware_properties: [android.os.IHardwarePropertiesManager]	122	media.camera: [android.hardware.ICameraService]
48	serial: [android.hardware.ISerialManager]	123	media.VTS: [android.hardware.IVTSERVICE]
49	usb: [android.hardware.usb.IUsbManager]	124	media.sound_trigger_hw: [android.hardware.ISoundTriggerHwService]
50	midi: [android.media.midi.IMidiManager]	125	media.radio: [android.hardware.IRadioService]
51	DockObserver: []	126	media.audio_policy: [android.media.IAudioPolicyService]
52	audio: [android.media.IAudioService]	127	drm.drmManager: [drm.IDrmManagerService]

53	wallpaper: [android.app.IWallpaperManager]	128	media.resource_manager: [android.media.IResourceManagerService]
54	dropbox: [com.android.internal.os.IDropBoxManagerService]	129	media.player: [android.media.IMediaPlayerService]
55	search_engine: [com.mediatek.search.ISearchEngineManagerService]	130	media.extractor: [android.media.IMediaExtractorService]
56	search: [android.app.ISearchManager]	131	media.drm: [android.media.IMediaDrmService]
57	country_detector: [android.location.ICountryDetector]	132	vivo_daemon.service: [IVivoDmService]
58	location: [android.location.ILocationManager]	133	media.audio_flinger: [android.media.IAudioFlinger]
59	devicestoragemonitor: []	134	media.servicehub: [com.vivo.media.IServiceHub]
60	notification: [android.app.INotificationManager]	135	media.codec: [android.media.IMediaCodecService]
61	recovery: [android.os.IRecoverySystem]	136	PQ: [PQService]
62	updatelock: [android.os.IUpdateLock]	137	android.hardware.fingerprint.IFingerprintDaemon: []
63	data_shaping: [com.mediatek.datashaping.IDataShapingManager]	138	android.service.gatekeeper.IGateKeeperService: []
64	servicediscovery: [android.net.nsd.INsdManager]	139	program_binary: []
65	connectivity: [android.net.IConnectivityManager]	140	android.security.keystore: [android.security.IKeystoreService]
66	ethernet: [android.net.IEthernetManager]	141	getuk.service: []
67	rttmanager: [android.net.wifi.IRttManager]	142	NvRAMAgent: [NvRAMAgent]
68	wifiscanner: [android.net.wifi.IWifiScanner]	143	mtk.codecservice: []
69	wifi: [android.net.wifi.IWifiManager]	144	android.hardware.fingerprint.IGoodixFingerprintDaemon: []
70	wifip2p: [android.net.wifi.p2p.IWifiP2pManager]	145	batteryproperties: [android.os.IBatteryPropertiesRegistrar]
71	netpolicy: [android.net.INetworkPolicyManager]	146	GuiExtService: [GuiExtService]
72	netstats: [android.net.INetworkStatsService]	147	gpu: [android.ui.IGpuService]
73	network_score: [android.net.INetworkScoreService]	148	SurfaceFlinger: [android.ui.ISurfaceComposer]
74	textservices: [com.android.internal.textservice.ITextServicesManager]		

Third Party Applications

Number of Third Party Applications installed on Device: 61

3rd Party Applications installed on Device-Vivo

com.google.android.apps.subscriptions.red	com.avenuegrowth
com.nestik.kalilinux	cc.blynk
com.truecaller	com.google.android.apps.nbu.files
com.indiainfoline	com.google.android.apps.classroom
com.nextbillion.groww	com.microsoft.office.word
com.vivo.easyshare	com.microsoft.office.powerpoint
com.sp.protector.free	ai.wizely.android
com.sololearn	com.saavn.android
com.myairtelapp	com.zhiliaoapp.musically
com.paprbit.dcoder	com.spotify.music
com.whatsapp	com.mventus.selfcare.activity
com.google.android.apps.docs.editors.sheets	com.application.zomato
com.microsoft.skydrive	com.udemy.android
com.flipkart.android	com.northpark.drinkwater
com.bitstrips.imoji	com.gaana
com.sonyliv	com.android.bbk.lockscreen3
com.confirmtkitlite	com.meetup
com.ryzac.codecademygo	srl.midnighttea.pushit
com.microsoft.launcher	com.adobe.reader
com.instagram.android	com.nike.ntc
com.microsoft.office.onenote	com.storybeat
com.hp.orbit	com.google.android.apps.nbu.paisa.user
in.startv.hotstar	com.cisco.webex.meetings
org.chromium.webapk.a879f9decdbdb68787	com.nexstreaming.app.kinemasterfree
com.mycaptain.app	com.goibibo
com.ionicframework.someapp771914	com.intsig.camscanner
com.microsoft.emmx	club.fromfactory
com.google.android.instantapps.supervisor	in.gov.swayam.app
com.olacabs.customer	no.mobitroll.kahoot.android
com.snapchat.android	cn.wps.moffice_eng

Section B. Malware Report

Malware Report of VIVO Device

DEVICENAME	APPNAME	SHA256	ENGINE1	ENGINE2	ENGINE3	ENGINE4	ENGINE5	ENGINE6	OVERALL
VIVO	AssamesePack.apk	5884cb86340fa20a753be404b5cddb47351e1a01fe14149bf19ffb107098cd4c	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	MalayalamPack.apk	4217e611014511062a1e8ac2df42253db505b96a66103ad3e9c8c20a0acd19dd	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	ZawgyiPack.apk	4905e9969ace0da9e4b0090aec88001e822e0d2c49feb510fbcc8d421f8a813a	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	VivoDreamMusicApp.apk	ee0a6e179984af8803f981f9ed20380cdecc9a072a7592eda8e153637921033b	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	ThaiPack.apk	a174739c7dd91d19cf89015cbce292649a8f5848eade5d0d6d806b3307a17793	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	GoogleExtServices.apk	de11eeb473f9371cb71c5adfe4e94c36ae4e600625ddc7c8dc50acb8a999e5bd	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	Compass.apk	fc2c4b9c7c1986939e24591d33d5a2113ca965dc86264ae0df88672886acbd7e	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	GameWatch.apk	847727a147c2899ea309462da7f87bea4f889fc55bd111c8ced20c7d1d169654	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	TamilPack.apk	ff92fd79efb69ff501a49b7646f4e504dacda296de54d050122436d8fba2cb89	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	VivoThemeRes.apk	165516d42c8b7558a2f0cce7f95cc31c2fe3d55054eebcc39a97f4a0bdfacc04	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	PunjabiPack.apk	c781a643fdedd930344b8028050915047832103dbccd9b4a28b6e1708d5f3151	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	VivoDreamNoteApp.apk	38364b50befa50d63676637973e3b907c04473fb479df54948b9125b1933db9	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	GujaratiPack.apk	9b11bda1bd259b9b2eb6cfa12f5b9ee6cccb0493f309820306c524f243653505	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	ManipuriPack.apk	93d806dfbabbd719c59e8693c072ea63e3daaa2f2062a60bbc86c5f0edb2f066	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	TelephonyProvider.apk	a6984b5b595fee31b22698cc54ca521c360800692a9344bd84319257d7d08b4ff	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	Silk.apk	6a1bc11a924d391cf9411b71b5a6c348fa2b1af567ad477922834a13d1372974	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	BBKPhoneInstructions.apk	69da4195ae3bb5a43ab45b9aa6b30a6eaf15d1e0d5b7e5a8c0a84310afd022ff	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	HindilatinPack.apk	4783420039937187f877a60b6adc9527fd76a23ab78d213bb6e5de471ad19ff7	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	IndiandogriPack.apk	bda4744ca8603ec2781b462a23a04ed88905a66fd89783f297d32a90a500721f	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	DoubleTimezoneClock.apk	0be6884bdd3b31997caa8141e653621b7bd60def0735c652e7eeb44cf96962af	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	FuelSummary.apk	fd05c78a905f58f22c2efbc265a93f39892a4a1c089d9f24f13cc76177639e49	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	VivoSetupWizard.apk	73ec1822ca61317634ef3db09987f8e5b1f375c5a6ead01e823c5dda1c0aedfd	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	MarathiPack.apk	341aa554422d4ad37c45eda4027f3cc635bb5dbeedd11b7f4d3eb2e8d75969b1	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	CameraParamLuma.apk	2a44b72bda8977e59a3b4332037a5453ab4a25452ad24d0bdbcafc08545b440e	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	BBKFMRadio.apk	8651f772d63c1eef8f6166fecf74dc5306fcb41c7bf691d011de7c851713a83	SAFE	SAFE	SAFE	MALWARE	SAFE	SAFE	MALWARE
VIVO	CoffeeTime.apk	e5c04c85090fe34a23dac155036dd315e021e922fa305807ed4daff74a614f23	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	IndiankonkaniknPack.apk	124b11bffb94f48d201df00a470fe97714e120d7e1a18b8a0878314de034d037	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	BengaliPack.apk	42f7fe0b03c3a74b604d08e3f563f62e5417c76273842b037ca0c3de9a0d52ef	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	MTKLOG.apk	63eeafae40b5b4bf49b4376cf2c811ba33581fb9a548acd5765d11fab0e13b37	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	KhmerPack.apk	59220eb34eedbccd0649b26e8add524aebb7a7375d90c935b11a52d5e79305ce	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	SpanishPack.apk	8541b91cca4f0e2e56587e7d16cedbdd89f6517165e88c6a310b1c65b3e6632b	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	ConfigUpdater.apk	a7bf812b312ec6ce4ac01b9c30abf5aac21c8fe82fe5baba60bf4ad7518c6951	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	SharedStorageBackup.apk	f8de08410801f6a73db61116feee14df81b3e125a14491caa2cabb04863af89d	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	BurmesePack.apk	3fabfbca497bfcb1771aed3443be7113d5749277c03e19898d3170fc625267a	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	EWarranty.apk	28c7c381058743c4e837293a326b0a0e54ea194ba9ec87dc407050c93a6c3a53	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	CtsShimPrebuilt.apk	bb5b66c98398ee368dda15001e6eaebba5ac32223d4a09466a1572c723f68ca0	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	OriyaPack.apk	57d270b1666f081d9fb9e7ecd7baae7d422dfe6407b0e3fe4933ca6dd81b2894	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	MusicSkinSpeaker.apk	a5077895ce21611eef5f8a2cf1725ad8585dc943290e31d1a0be4469efaf0046	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	SomaliPack.apk	8c7cbf1242c07d9ef0d55c33bfc13e33ebc8068b756d475b29c2fbe5d391b650	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	BrowserActivity.apk	36817aa74ab0e454296b45f0fa988e36292117d7b8bd411a8647811f0dd7fb00	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	IndonesianPack.apk	f426b5b22683cfd1f11f659b27a534bca872fe693399d3bd29ecff34fd26dd55	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	BluetoothMidiService.apk	b0e4b853bbd78820aa03ee8b4a92563bd74292e385be8193647ac83b372cf47d	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	MalayanPack.apk	29ad430ce4188c709e0649f514b7c8847562e5e648cfdcd498037d6d9fcc2d1a	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	CoralSea.apk	b45466c8548394e03154aa2b9fc0e4a8107f7e46bd4811ca580038c77076eb93	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	PartnerBookmarksProvider.apk	b847ba9153582b3a2db2f785b8993d731687a59b2bd4a6d272bd8810e44d69a4	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	YGPS.apk	c3098483f3fa3adae0199334e12fc0c90a411d1b5ddf1c9a5ff597522a0d0514	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	TagalogPack.apk	683cb61cfcf2b45cef63fbdfa331f4b7269246d6e30a7a77d59e906e91d24056	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	HinglishPack.apk	89c2539b8e070cd2e47cc724c8ca1415427eb4e45e0cebb865338f73031546b9	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	BBKMusicEffectTest.apk	fecb8628dbd88eb693b762d8af56fc6220c050f9a9ac683dc32c30c8d80ba24b	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	WfoService.apk	bfedfd2d70fa001b4577ba9804bf32b527617f751d487f2bef25dc50178a4ebd	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	VivoLogUpdate.apk	822abb0607df638e3b83dd0700e8ad797b3e4cc56b8d49365fff5c40b85c6922	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	MiraVision.apk	d165e54244940b07032a4eee6ebdc5e1272579ab30cd22a29fc65e5c16acd2ac	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	KannadaPack.apk	151f3e34dae46004d3d4c1b361f54e728b2afbb62ca26c80af5917ce05d53f9a	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	WebViewGoogle.apk	2f006408b5e54108ea4b6ce6866e8c4f687c2f2d17135732ee614fd740b1a0de	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	InputDevices.apk	32efd6a32c1b7baddd1aa1488daa3fc3c7eee94ae5064b5be35fe33219e166ca	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
VIVO	MediaTune.apk	134f46ad5b24f4778f0ef1a0e9229212d3de123af303bf61df8d64e866bd0a0f	SAFE	SAFE	SAFE	MALWARE	SAFE	SAFE	MALWARE

Section C. CVE Report

CVE Report of VIVO Device

Name	Description
CVE-2019-5876	Use after free in media in Google Chrome on Android prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5833	Incorrect dialog box scoping in browser in Google Chrome on Android prior to 75.0.3770.80 allowed a remote attacker to display misleading security UI via a crafted HTML page.
CVE-2019-5816	Process lifetime issue in Chrome in Google Chrome on Android prior to 74.0.3729.108 allowed a remote attacker to potentially persist an exploited process via a crafted HTML page.
CVE-2019-5767	Insufficient protection of permission UI in WebAPKs in Google Chrome on Android prior to 72.0.3626.81 allowed an attacker who convinced the user to install a malicious application to access privacy/security sensitive web APIs via a crafted APK.
CVE-2019-5765	An exposed debugging endpoint in the browser in Google Chrome on Android prior to 72.0.3626.81 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted Intent.
CVE-2019-5759	Incorrect lifetime handling in HTML select elements in Google Chrome on Android and Mac prior to 72.0.3626.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2019-13707	Insufficient validation of untrusted input in intents in Google Chrome on Android prior to 78.0.3904.70 allowed a local attacker to leak files via a crafted application.
CVE-2019-13703	Insufficient policy enforcement in the Omnibox in Google Chrome on Android prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13695	Use after free in audio in Google Chrome on Android prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6057	Lack of special casing of Android ashmem in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to bypass inter-process read only guarantees via a crafted HTML page.
CVE-2018-18353	Failure to dismiss http auth dialogs on navigation in Network Authentication in Google Chrome on Android prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of an auto dialog via a crafted HTML page.
CVE-2017-5120	Inappropriate use of www mismatch redirects in browser navigation in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to potentially downgrade HTTPS requests to HTTP via a crafted HTML page.
CVE-2017-5119	Use of an uninitialized value in Skia in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5118	Blink in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, failed to correctly propagate CSP restrictions attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5116	Type confusion in V8 in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5114	Inappropriate use of partition alloc in PDFium in Google Chrome prior to 61.0.3163.79 for Linux, Windows, and Mac, and 61.0.3163.81 for Android, allowed a remote attacker to potentially exploit memory corruption via a crafted PDF file.
CVE-2017-5113	Math overflow in Skia in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5110	Inappropriate implementation of the web payments API on blob: and data: schemes in Web Payments in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to spoof the contents of the Omnibox via a crafted HTML page.
CVE-2017-5108	Type confusion in PDFium in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to potentially maliciously modify objects via a crafted PDF file.
CVE-2017-5106	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5105	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5102	Use of an uninitialized value in Skia in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5098	A use after free in V8 in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5096	Insufficient policy enforcement during navigation between different schemes in Google Chrome prior to 60.0.3112.78 for Android allowed a remote attacker to perform cross origin content download via a crafted HTML page, related to intents.
CVE-2017-5094	Type confusion in extensions JavaScript bindings in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to potentially maliciously modify objects via a crafted HTML page.
CVE-2017-5093	Inappropriate implementation in modal dialog handling in Blink in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to prevent a full screen warning from being displayed via a crafted HTML page.
CVE-2017-5091	A use after free in IndexedDB in Google Chrome prior to 60.0.3112.78 for Linux, Android, Windows, and Mac allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5088	Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.104 for Mac, Windows, and Linux, and 59.0.3071.117 for Android, allowed a remote

	attacker to perform out of bounds memory access via a crafted HTML page.
CVE-2017-5087	A use after free in Blink in Google Chrome prior to 59.0.3071.104 for Mac, Windows, and Linux, and 59.0.3071.117 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page, aka an IndexedDB sandbox escape.
CVE-2017-5083	Inappropriate implementation in Blink in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.
CVE-2017-5082	Failure to take advantage of available mitigations in credit card autofill in Google Chrome prior to 59.0.3071.92 for Android allowed a local attacker to take screen shots of credit card information via a crafted HTML page.
CVE-2017-5081	Lack of verification of an extension's locale folder in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed an attacker with local write access to modify extensions by modifying extension files.
CVE-2017-5079	Inappropriate implementation in Blink in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.
CVE-2017-5077	Insufficient validation of untrusted input in Skia in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5076	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5075	Inappropriate implementation in CSP reporting in Blink in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to obtain the value of url fragments via a crafted HTML page.
CVE-2017-5073	Use after free in print preview in Blink in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5072	Inappropriate implementation in Omnibox in Google Chrome prior to 59.0.3071.92 for Android allowed a remote attacker to perform domain spoofing with RTL characters via a crafted URL page.
CVE-2017-5071	Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows and Mac, and 59.0.3071.92 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5070	Type confusion in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-5069	Incorrect MIME type of XSS-Protection reports in Blink in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to circumvent Cross-Origin Resource Sharing checks via a crafted HTML page.
CVE-2017-5066	Insufficient consistency checks in signature handling in the networking stack in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to incorrectly accept a badly formed X.509 certificate via a crafted HTML page.
CVE-2017-5063	A numeric overflow in Skia in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5062	A use after free in Chrome Apps in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to potentially perform out of bounds memory access via a crafted Chrome extension.
CVE-2017-5060	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5059	Type confusion in Blink in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to potentially obtain code execution via a crafted HTML page.
CVE-2017-5057	Type confusion in PDFium in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2017-5056	A use after free in Blink in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5054	An out-of-bounds read in V8 in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to obtain heap memory contents via a crafted HTML page.
CVE-2017-5053	An out-of-bounds read in V8 in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page, related to Array.prototype.indexOf.
CVE-2017-5052	An incorrect assumption about block structure in Blink in Google Chrome prior to 57.0.2987.133 for Mac, Windows, and Linux, and 57.0.2987.132 for Android, allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page that triggers improper casting.
CVE-2017-5051	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5050	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5049	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5048	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5047	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5046	V8 in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android had insufficient policy enforcement, which allowed a remote attacker to spoof the location object via a crafted HTML page, related to Blink information disclosure.
CVE-2017-5045	XSS Auditor in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed detection of a blocked iframe load, which allowed a remote attacker to brute force JavaScript variables via a crafted HTML page.
CVE-2017-5044	Heap buffer overflow in filter processing in Skia in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5042	Cast in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android sent cookies to sites discovered via SSDP, which allowed an attacker on the local network segment to initiate connections to arbitrary URLs and observe any plaintext cookies sent.
CVE-2017-5040	V8 in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android was missing a neutering check, which allowed a remote attacker

	to read values in memory via a crafted HTML page.
CVE-2017-5039	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5037	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5036	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to have an unspecified impact via a crafted PDF file.
CVE-2017-5033	Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android failed to correctly propagate CSP restrictions to local scheme pages, which allowed a remote attacker to bypass content security policy via a crafted HTML page, related to the unsafe-inline keyword.
CVE-2017-5030	Incorrect handling of complex species in V8 in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac and 57.0.2987.108 for Android allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2017-5029	The xsltAddTextString function in transform.c in libxslt 1.1.29, as used in Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android, lacked a check for integer overflow during a size calculation, which allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2017-5027	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy , which allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2017-5023	Type confusion in Histogram in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit a near null dereference via a crafted HTML page.
CVE-2017-5022	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2017-5021	A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5020	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to require a user gesture for powerful download operations , which allowed a remote attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted HTML page.
CVE-2017-5019	A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5018	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, had an insufficiently strict content security policy on the Chrome app launcher page, which allowed a remote attacker to inject scripts or HTML into a privileged page via a crafted HTML page.
CVE-2017-5016	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to prevent certain UI elements from being displayed by non-visible pages, which allowed a remote attacker to show certain UI elements on a page they don't control via a crafted HTML page.
CVE-2017-5015	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled Unicode glyphs, which allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5014	Heap buffer overflow during image processing in Skia in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5012	A heap buffer overflow in V8 in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5010	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, resolved promises in an inappropriate context, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5009	WebRTC in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5008	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed attacker controlled JavaScript to be run during the invocation of a private script method, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5007	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled the sequence of events when closing a page, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5006	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled object owner relationships, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-9650	Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled iframes, which allowed a remote attacker to bypass a no-referrer policy via a crafted HTML page.
CVE-2016-5225	Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled form actions, which allowed a remote attacker to bypass Content Security Policy via a crafted HTML page.
CVE-2016-5224	A timing attack on denormalized floating point arithmetic in SVG filters in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.
CVE-2016-5223	Integer overflow in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption or DoS via a crafted PDF file.
CVE-2016-5222	Incorrect handling of invalid URLs in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2016-5221	Type confusion in libGLESv2 in ANGLE in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android possibly allowed a remote attacker to bypass buffer validation via a crafted HTML page.
CVE-2016-5220	PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to read local files via a crafted PDF file.
CVE-2016-5219	A heap use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5218	The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to temporarily spoof the contents of the Omnibox (URL bar) via a crafted HTML page containing PDF data.
CVE-2016-5217	The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly permitted access to privileged plugins, which allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2016-5216	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to performan

	out of bounds memory read via a crafted PDF file.
CVE-2016-5215	A use after free in webaudio in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2016-5213	A use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5212	Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android insufficiently sanitized DevTools URLs, which allowed a remote attacker to read local files via a crafted HTML page.
CVE-2016-5211	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5210	Heap buffer overflow during TIFF image parsing in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5209	Bad casting in bitmap manipulation in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5208	Blink in Google Chrome prior to 55.0.2883.75 for Linux and Windows, and 55.0.2883.84 for Android allowed possible corruption of the DOM tree during synchronous event handling, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5207	In Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android, corruption of the DOM tree could occur during the removal of a full screen element, which allowed a remote attacker to achieve arbitrary code execution via a crafted HTML page.
CVE-2016-5206	The PDF plugin in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly followed redirects, which allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.
CVE-2016-5204	Leaking of an SVG shadow tree leading to corruption of the DOM tree in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5203	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5200	V8 in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android incorrectly applied type rules, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5199	An off by one error resulting in an allocation of zero size in FFmpeg in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2016-5198	V8 in Google Chrome prior to 54.0.2840.90 for Linux, and 54.0.2840.85 for Android, and 54.0.2840.87 for Windows and Mac included incorrect optimisation assumptions, which allowed a remote attacker to perform arbitrary read/write operations, leading to code execution, via a crafted HTML page.
CVE-2016-5197	The content view client in Google Chrome prior to 54.0.2840.85 for Android insufficiently validated intent URLs, which allowed a remote attacker who had compromised the renderer process to start arbitrary activity on the system via a crafted HTML page.
CVE-2016-5196	The content renderer client in Google Chrome prior to 54.0.2840.85 for Android insufficiently enforced the Same Origin Policy amongst downloaded files, which allowed a remote attacker to access any downloaded file and interact with sites, including those the user was logged into, via a crafted HTML page.
CVE-2016-5191	Bookmark handling in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation of supplied data, allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages
CVE-2016-5190	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles during shutdown, which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.
CVE-2016-5189	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted navigation to blob URLs with non-canonical origins, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.
CVE-2016-5187	Google Chrome prior to 54.0.2840.85 for Android incorrectly handled rapid transition into and out of full screen mode, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.
CVE-2016-5186	Devtools in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled objects after a tab crash, which allowed a remote attacker to perform an out of bounds memory read via crafted PDF files.
CVE-2016-5185	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly allowed reentrance of FrameView ::updateLifecyclePhasesInternal(), which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.
CVE-2016-5184	PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles in CFFL_FormFiller::KillFocusForAnnot, which allowed a remote attacker to potentially exploit heap corruption via crafted PDF files.
CVE-2016-5183	A heap use after free in PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android allows a remote attacker to potentially exploit heap corruption via crafted PDF files.
CVE-2016-5182	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation in bitmap handling, which allowed a remote attacker to potentially exploit heap corruption via crafted HTML pages.
CVE-2016-5181	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted execution of v8 microtasks while the DOM was in an inconsistent state, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages.
CVE-2016-5163	The bidirectional-text implementation in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not ensure left-to-right (LTR) rendering of URLs, which allows remote attackers to spoof the address bar via crafted right-to-left (RTL) Unicode text, related to omnibox/SuggestionView.java in Chrome for Android.
CVE-2016-1671	Google Chrome before 50.0.2661.102 on Android mishandles / (slash) and \ (backslash) characters, which allows attackers to conduct directory traversal attacks via a file: URL, related to net/base/escape.cc and net/base/filename_util.cc.
CVE-2016-1656	The download implementation in Google Chrome before 50.0.2661.75 on Android allows remote attackers to bypass intended pathname restrictions via unspecified vectors.
CVE-2016-0959	Use after free vulnerability in Adobe Flash Player Desktop Runtime before 20.0.0.267, Adobe Flash Player Extended Support Release before 18.0.0.324, Adobe Flash Player for Google Chrome before 20.0.0.267, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 before 20.0.0.267, Adobe Flash Player for Internet Explorer 10 and 11 before 20.0.0.267, Adobe Flash Player for Linux before 11.2.202.559, AIR Desktop Runtime before 20.0.0.233, AIR SDK before 20.0.0.233, AIR SDK & Compiler before 20.0.0.233, AIR for Android before 20.0.0.233.
CVE-2015-6783	The FindStartOffsetOfFileInZipFile function in crazy_linker_zip.cpp in crazy_linker (aka Crazy Linker) in Android 5.x and 6.x, as used in Google Chrome before 47.0.2526.73, improperly searches for an EOCD record, which allows attackers to bypass a signature-validation requirement via a crafted ZIP archive.
CVE-2015-2239	Google Chrome before 41.0.2272.76, when Instant Extended mode is used, does not properly consider the interaction between the "1993 search" features and restore-from-disk RELOAD transitions, which makes it easier for remote attackers to spoof the address bar for a search-results page by leveraging a compromised search engine
CVE-2015-1275	Cross-site scripting (XSS) vulnerability in org/chromium/chrome/browser/UrlUtilities.java in Google Chrome before 44.0.2403.89 on Android allows remote attackers to inject

CVE-2015-1261	arbitrary web script or HTML via a crafted intent: URL, as demonstrated by a trailing alert(document.cookie);// substring, aka "Universal XSS (UXSS)."
CVE-2015-1212	android/java/src/org/chromium/chrome/browser/WebsiteSettingsPopup.java in Google Chrome before 43.0.2357.65 on Android does not properly restrict use of a URL's fragment identifier during construction of a page-info popup, which allows remote attackers to spoof the URL bar or deliver misleading popup content via crafted text.
CVE-2015-1211	Multiple unspecified vulnerabilities in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1210	The OriginCanAccessServiceWorkers function in content/browser/service_worker/service_worker_dispatcher_host.cc in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android does not properly restrict the URI scheme during a ServiceWorker registration
CVE-2015-1209	The V8ThrowException::createDOMException function in bindings/core/v8/V8ThrowException.cpp in the V8 bindings in Blink, as used in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android, does not properly consider frame access restrictions during the throwing of an exception
CVE-2014-9648	Use-after-free vulnerability in the VisibleSelection::nonBoundaryShadowTreeNode function in core/editing/VisibleSelection.cpp in the DOM implementation in Blink , as used in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android, allows remote attackers to cause a denial of service
CVE-2014-7905	components/navigation_interception/intercept_navigation_resource_throttle.cc in Google Chrome before 40.0.2214.91 on Android does not properly restrict use of intent: URLs to open an application after navigation to a web site, which allows remote attackers to cause a denial of service (loss of browser access to that site) via crafted JavaScript code
CVE-2014-3201	Google Chrome before 39.0.2171.65 on Android does not prevent navigation to a URL in cases where an intent for the URL lacks CATEGORY_BROWSABLE, which allows remote attackers to bypass intended access restrictions via a crafted web site.
CVE-2014-3166	core/rendering/compositing/RenderLayerCompositor.cpp in Blink, as used in Google Chrome before 38.0.2125.102 on Android, does not properly handle a certain IFRAME overflow condition, which allows remote attackers to spoof content via a crafted web site that interferes with the scrollbar.
CVE-2014-3161	The Public Key Pinning (PKP) implementation in Google Chrome before 36.0.1985.143 on Windows, OS X, and Linux, and before 36.0.1985.135 on Android, does not correctly consider the properties of SPDY connections, which allows remote attackers to obtain sensitive information by leveraging the use of multiple domain names.
CVE-2014-3159	The WebMediaPlayerAndroid::load function in content/renderer/media/android/webmediaplayer_android.cc in Google Chrome before 36.0.1985.122 on Android does not properly interact with redirects, which allows remote attackers to bypass the Same Origin Policy via a crafted web site that hosts a video stream.
CVE-2013-6642	The WebContentsDelegateAndroid::OpenURLFromTab function in components/web_contents_delegate_android/web_contents_delegate_android.cc in Google Chrome before 36.0.1985.122 on Android does not properly restrict URL loading, which allows remote attackers to spoof the URL in the Omnibox via unspecified vectors.
CVE-2012-4909	Google Chrome through 32.0.1700.23 on Android allows remote attackers to spoof the address bar via unspecified vectors.
CVE-2012-4908	Google Chrome before 18.0.1025308 on Android allows remote attackers to obtain cookie information via a crafted application.
CVE-2012-4907	Google Chrome before 18.0.1025308 on Android allows remote attackers to bypass the Same Origin Policy and obtain access to local files via vectors involving a symlink.
CVE-2012-4906	Google Chrome before 18.0.1025308 on Android does not properly restrict access from JavaScript code to Android APIs, which allows remote attackers to have an unspecified impact via a crafted web page.
CVE-2012-4905	Google Chrome before 18.0.1025308 on Android does not properly restrict access to file: URLs, which allows remote attackers to obtain sensitive information via unspecified vectors, as demonstrated by obtaining credential data, a different vulnerability than CVE-2012-4903.
CVE-2012-4904	Cross-site scripting (XSS) vulnerability in Google Chrome before 18.0.1025308 on Android allows remote attackers to inject arbitrary web script or HTML via an extra in an Intent object, aka "Universal XSS (UXSS)."
CVE-2012-4903	Cross-application scripting vulnerability in Google Chrome before 18.0.1025308 on Android allows remote attackers to inject arbitrary web script via unspecified vectors , as demonstrated by "Universal XSS (UXSS)" attacks against the current tab.
CVE-2011-3881	Google Chrome before 18.0.1025308 on Android does not properly restrict access to file: URLs, which allows remote attackers to obtain sensitive information via unspecified vectors, as demonstrated by obtaining credential data, a different vulnerability than CVE-2012-4906.
CVE-2009-1442	WebKit, as used in Google Chrome before 15.0.874.102 and Android before 4.4, allows remote attackers to bypass the Same Origin Policy and conduct Universal XSS (UXSS) attacks
CVE-2019-3568	Multiple integer overflows in Skia, as used in Google Chrome 1.x before 1.0.154.64 and 2.x, and possibly Android, might allow remote attackers to execute arbitrary code in the renderer process via a crafted (1) image or (2) canvas.
CVE-2019-3566	A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of RTCP packets sent to a target phone number. The issue affects WhatsApp for Android prior to v2.19.134, WhatsApp Business for Android prior to v2.19.44, WhatsApp for iOS prior to v2.19.51, WhatsApp Business for iOS prior to v2.19.51, WhatsApp for Windows Phone prior to v2.18.348, and WhatsApp for Tizen prior to v2.18.15.
CVE-2019-11933	A bug in WhatsApp for Android's messaging logic would potentially allow a malicious individual who has taken over over a WhatsApp user's account to recover previously sent messages. This behavior requires independent knowledge of metadata for previous messages, which are not available publicly. This issue affects WhatsApp for Android 2.19.52 and 2.19.54 - 2.19.103, as well as WhatsApp Business for Android starting in v2.19.22 until v2.19.38.
CVE-2019-11932	A heap buffer overflow bug in libpl_droidsonroids_gif before 1.2.19, as used in WhatsApp for Android before version 2.19.291 could allow remote attackers to execute arbitrary code or cause a denial of service.
CVE-2019-11931	A double free vulnerability in the DDGifSlurp function in decoding.c in libpl_droidsonroids_gif before 1.2.15, as used in WhatsApp for Android before 2.19.244, allows remote attackers to execute arbitrary code or cause a denial of service.
CVE-2019-11927	A stack-based buffer overflow could be triggered in WhatsApp by sending a specially crafted MP4 file to a WhatsApp user. The issue was present in parsing the elementary stream metadata of an MP4 file and could result in a DoS or RCE. This affects Android versions prior to 2.19.274, iOS versions prior to 2.19.100, Enterprise Client versions prior to 2.25.3, Business for Android versions prior to 2.19.104 and Business for iOS versions prior to 2.19.100.
CVE-2018-6350	An integer overflow in WhatsApp media parsing libraries allows a remote attacker to perform an out-of-bounds write on the heap via specially-crafted EXIF tags in WEBP images. This issue affects WhatsApp for Android before version 2.19.143 and WhatsApp for iOS before version 2.19.100.
CVE-2018-6349	An out-of-bounds read was possible in WhatsApp due to incorrect parsing of RTP extension headers. This issue affects WhatsApp for Android prior to 2.18.276, WhatsApp Business for Android prior to 2.18.99, WhatsApp for iOS prior to 2.18.100.6, WhatsApp Business for iOS prior to 2.18.100.2, and WhatsApp for Windows Phone prior to 2.18.224.
CVE-2018-6344	When receiving calls using WhatsApp for Android, a missing size check when parsing a sender-provided packet allowed for a stack-based overflow. This issue affects WhatsApp for Android prior to 2.18.248 and WhatsApp Business for Android prior to 2.18.132.
CVE-2018-6339	A heap corruption in WhatsApp can be caused by a malformed RTP packet being sent after a call is established. The vulnerability can be used to cause denial of service. It affects WhatsApp for Android prior to v2.18.293, WhatsApp for iOS prior to v2.18.93, and WhatsApp for Windows Phone prior to v2.18.172.

	Business for Android starting in version v2.18.103 and was fixed in version v2.18.150.
CVE-2017-8769	** DISPUTED ** Facebook WhatsApp Messenger before 2.16.323 for Android uses the SD card for cleartext storage of files (Audio, Documents, Images, Video, and Voice Notes) associated with a chat, even after that chat is deleted. There may be users who expect file deletion to occur upon chat deletion, or who expect encryption (consistent with the application's use of an encrypted database to store chat text). NOTE: the vendor reportedly indicates that they do not "consider these to be security issues" because a user may legitimately want to preserve any file for use "in other apps like the Google Photos gallery" regardless of whether its associated chat is deleted.
CVE-2019-14319	The TikTok (formerly Musical.ly) application 12.2.0 for Android and iOS performs unencrypted transmission of images, videos, and likes. This allows an attacker to extract private sensitive information by sniffing network traffic.
CVE-2016-0959	Use after free vulnerability in Adobe Flash Player Desktop Runtime before 20.0.0.267, Adobe Flash Player Extended Support Release before 18.0.0.324, Adobe Flash Player for Google Chrome before 20.0.0.267, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 before 20.0.0.267, Adobe Flash Player for Internet Explorer 10 and 11 before 20.0.0.267, Adobe Flash Player for Linux before 11.2.202.559, AIR Desktop Runtime before 20.0.0.233, AIR SDK before 20.0.0.233, AIR SDK & Compiler before 20.0.0.233, AIR for Android before 20.0.0.233.
CVE-2014-6834	The Instaroid - Instagram Viewer (aka net.muik.instaroid) application 1.2.1 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2014-6690	The InstaMessage - Instagram Chat (aka com.futurebits.instagram.free) application 1.6.2 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2014-6007	The LikeHero Get Instagram Likes (aka com.fraoula.likehero) application 1.0.7 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2014-5679	The PopU 2: Get Likes on Instagram (aka com.popuapp.popu) application 1.7.5 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2014-5675	The Phonegram - Instagram Download (aka com.pinssible.padgram) application 1.9.5 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2014-5643	The Instachat -Instagram Messenger (aka com.instachat.android) application 1.6.2 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2014-5622	The Follow Mania for Instagram (aka com.followmania) application 1.2.1 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2014-5585	The Like4Like: Get Instagram Likes (aka com.bepop.bepop) application 2.1.5 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

Section D. Suggestion Report

SUGGESTION FOR UPDATION OF APPS

*KINDLY UPDATE THE APPS ON YOUR DEVICE FOR WHICH VERSION VARIOUS WITH DEVICE

App Name	Version
Adobe Acrobat Reader: PDF Viewer, Editor & Creator	19.9.2
Airtel Thanks - Recharge, Bill Pay, Bank, Live TV	4.4.16.4
AppLock - Fingerprint	7.4.2
Avenue Growth	2.9
CamScanner - Scanner to scan PDF	5.15.5.20191226
Cisco Webex Meetings	39.11.0
Club Factory - Online Shopping App	6.1.2
Dcoder, Compiler IDE :Code & Programming on mobile	2.1.6
Gaana Music - Hindi Tamil Telugu MP3 Songs Online	8.2.0
Goibibo - Hotel Car Flight IRCTC Train Bus Booking	7.6.8
Google	Varies with device
Google Classroom	Varies with device
Google Drive	Varies with device
Google Photos	Varies with device
Google Play Movies & TV	Varies with device
Google Sheets	Varies with device
Instagram	Varies with device
IRCTC train Booking, Indian Rail Train PNR Status	7.2.3
Meetup:Find events near you	3.21.15
Microsoft Edge	44.11.4.4121
Microsoft OneDrive	Varies with device
Ola Cabs - Book Taxi & Auto	5.0.5
Snapchat	10.72.5.0
SonyLIV -TV Shows, Movies & Live Sports Online,T20	5.4.1
Spotify: Listen to your favourite music & podcasts	8.5.36.747

Storybeat, unleash your creativity	1.3.3
Swayam	2.6.0
Truecaller: Caller ID, SMS, spam block & payments	10.61.9
Water Drink Reminder	Varies with device
WhatsApp Messenger	Varies with device
YouTube	Varies with device

Suggestion for Deletion of Apps

Appilication name
BBKFMRadio.
MediaTune.
Shell.
VLife_vivo.
GoogleBackupTransport.
BSPTest.
BackupRestoreConfirmation.