

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=4

A3. THIRD PARTY APPLICATIONS..... PAGE NO=5

SECTION B. MALWARE REPORT..... PAGE NO=6

B1. MALWARE REPORT OF THE DEVICEPAGE NO=6

SECTION C. CVE REPORT..... PAGE NO=8

C1. CVE REPORT OF THE DEVICE..... PAGE NO=8

SECTION D. SUGGESTIONS..... PAGE NO=13

D1. OUTDATED VERSION APPLICATIONS REPORT..... PAGE NO=13

D2. SUGGESTION (DELETE,UPDATE APPS) REPORT... PAGE NO=13

PACER: Threat Intelligence Report (TIR)

Section A. DEVICE INFORMATION

Information Of Device

Date: 08-01-20

Device Name: Samsung (52002296caf4765d)

Product: a2coreltd

Model number: SM-A260G

Device: a2corelte

transport_id: 5

RAM: Total Space= 1.00GB

Storage Capacity: Total Space= 16GB; Available Space=8.1GB

Android version: 8.1.0

Android Security Patch level: 2019-08-01

Software version : SMR Aug-2019 Release 1

Baseband version: A260GDDU2ASG2

version : 3.18.91-1637762-QB25063798

Build number : OPR6.A260GDD2ASG5

Applications Installed

Number of Applications installed on Device: 179

Applications installed on the Device-Samsung

com.sec.android.app.DataCreate	com.sec.android.inputmethod
com.android.cts.priv.ctsshim	com.sec.android.app.clock
com.samsung.android.smartswitchassistant	com.sec.android.RilServiceModeApp
com.sec.android.app.chromecustomizations	com.google.android.webview
com.google.android.ext.services	com.sec.android.app.simsettingmgr
com.android.providers.telephony	com.android.server.telecom
com.sec.android.app.parser	com.google.android.syncadapters.contacts
com.samsung.android.calendar	com.sec.imslogger
com.android.providers.calendar	com.fss.mobilepay.obc
com.osp.app.signin	com.android.keychain
com.sec.automation	com.android.chrome
com.android.providers.media	com.ovelin.guitartuna
com.google.android.onetimeinitializer	com.google.android.installer
com.google.android.ext.shared	com.google.android.gms
com.android.wallpapercropper	com.google.android.gsf
com.samsung.max.go	com.google.android.tts
com.google.android.apps.mapslite	com.android.calllogbackup
com.sec.factory.camera	com.google.android.partnersetup
com.sec.usbsettings	com.sec.spp.push
com.android.documentsui	com.android.carrierdefaultapp
android.auto_generated_rro____	com.android.proxyhandler
com.android.externalstorage	com.sec.android.app.launcher
com.sec.factory	net.rention.mind.skillz
com.android.htmlviewer	com.google.android.feedback
com.android.companiondevicemanager	com.google.android.printservice.recommendation

com.google.android.apps.navlite
com.android.mms.service
com.android.providers.downloads
com.wsomacp
com.samsung.android.MtpApplication
com.sec.android.app.factorykeystring
com.sec.android.app.samsungapps
com.sec.android.emergencymode.service
com.google.android.configupdater
com.sec.android.app.wlantest
com.sec.epdgtestapp
com.android.defcontainer
com.sec.ims
com.sec.sve
com.android.providers.downloads.ui
com.android.vending
com.android.pacprocessor
com.google.android.gm.lite
com.sec.android.provider.badge
com.android.certinstaller
com.android.carrierconfig
android
com.android.contacts
com.android.egg
com.android.mtp
com.android.stk
com.samsung.android.messaging
com.android.backupconfirm
com.amazon.dee.app
com.hdwallpaper.wallpaper
com.sec.android.app.SecSetupWizard
com.android.statementservice
com.yaantraportal.app
com.sec.android.app.sbrowser.lite
com.google.android.apps.tachyon
com.sec.android.app.hwmoduletest
com.sec.bcservice
com.sec.modem.settings
com.android.systemui.theme.dark
com.google.android.apps.searchlite
com.sec.android.app.sysscope
com.sec.android.app.wallpaperchooser
com.samsung.android.providers.context
com.sec.android.app.servicemodeapp
com.sec.android.preloadinstaller
com.google.android.setupwizard
com.sec.android.gallery3d
com.android.providers.settings
com.sec.imsservice
com.android.sharedstoragebackup
com.facebook.services
com.google.android.music
com.android.printspooler
com.android.dreams.basic
com.android.incallui
com.android.inputdevices
com.samsung.android.kgclient
com.android.bips
com.android.stk2
com.google.android.apps.nbu.files
com.samsung.android.timezone.autoupdate_O
com.google.android.apps.docs
com.samsung.advp.imssettings
net.one97.paytm

com.samsung.adaptivebrightnessgo
com.google.android.apps.photos
com.google.android.syncadapters.calendar
com.android.managedprovisioning
com.spotify.music
com.acr.androiddownloadmanager
com.samsung.safetyinformation
com.sec.android.app.ringtoneBR
com.google.android.apps.speechservices
com.mgs.obcbank
com.android.providers.partnerbookmarks
com.facebook.lite
com.facebook.system
com.sec.android.app.popupcalculator
com.sec.android.soagent
com.sec.unifiedwfc
com.sec.phone
org.edx.mobile
com.samsung.app.samsungmemberstub
com.google.android.backuptransport
com.android.storagemanager
com.android.bookmarkprovider
com.android.settings
com.google.android.apps.nbu.paisa.user
com.sec.android.app.bluetoothtest
com.hdw.blackwallpapers
com.sec.android.emergencylauncher
com.google.android.apps.books
com.android.cts.ctsshim
com.aura.oobe.samsung
com.samsung.android.svcagent
com.google.android.apps.assistant
com.unacademyapp
com.android.vpndialogs
com.samsung.memorysaver
com.android.phone
com.android.shell
com.android.wallpaperbackup
com.android.providers.blockednumber
com.android.providers.userdictionary
com.wssyncmldm
in.swiggy.android
com.android.location.fused
com.sec.epdg
com.android.systemui
com.sec.android.app.personalization
com.google.android.apps.youtube.mango
com.android.bluetoothmidiservice
com.sec.rrocentre
com.kiloo.subwaysurf
com.facebook.appmanager
com.samsung.logwriter
com.sec.android.app.fm
com.sec.android.provider.emergencymode
com.google.android.play.games
com.sec.android.app.camera
com.android.bluetooth
com.android.providers.contacts
com.sec.android.widgetapp.webmanual
com.samsung.sec.android.application.csc
com.android.captiveportallogin
com.google.android.inputmethod.latin
com.samsung.android.sm.go
com.samsung.android.video

Services Running On The Device

Number of services running on Device: **144** services

List of Services Running On the Device-Samsung

0	textSDUFSService.unionFSStackService: []	72	CustomFrequencyManagerService: [android.os.ICustomFrequencyManager]
1	ims6: [com.samsung.android.ims.ISemImsService]	73	persistent_data_block: [android.service.persistentdata.IPersistentDataBlockService]
2	secims: [com.sec.ims.IImsService]	74	lock_settings: [com.android.internal.widget.ILockSettings]
3	epdgService: [com.sec.epdg.IEpdgManager]	75	uimode: [android.app.IUiModeManager]
4	ims: [com.android.ims.internal.IImsService]	76	motion_recognition: [com.samsung.android.gesture.IMotionRecognitionService]
5	carrier_config: [com.android.internal.telephony.ICarrierConfigLoader]	77	storagestats: [android.app.usage.IStorageStatsManager]
6	phone: [com.android.internal.telephony.ITelephony]	78	mount: [android.os.storage.IStorageManager]
7	isms: [com.android.internal.telephony.ISms]	79	FMPlayer: [com.samsung.android.media.fmradio.internal.IFMPlayer]
8	iphonesubinfo: [com.android.internal.telephony.IPhoneSubInfo]	80	accessibility: [android.view.accessibility.IAccessibilityManager]
9	simphonebook: [com.android.internal.telephony.IIccPhoneBook]	81	input_method: [com.android.internal.view.IInputMethodManager]
10	telecom: [com.android.internal.telecom.ITelecomService]	82	pinner: []
11	isub: [com.android.internal.telephony.ISub]	83	vrmanager: [android.service.vr.IVrManager]
12	SveService: []	84	input: [android.hardware.input.IInputManager]
13	emergency_service: []	85	window: [android.view.IWindowManager]
14	contexthub: [android.hardware.location.IContextHubService]	86	alarm: [android.app.IAlarmManager]
15	netd_listener: [android.net.metrics.INetdEventListener]	87	consumer_ir: [android.hardware.IConsumerIrService]
16	connmetrics: [android.net.IIpConnectivityMetrics]	88	vibrator: [android.os.IVibratorService]
17	bluetooth_manager: [android.bluetooth.IBluetoothManager]	89	settings: []
18	autofill: [android.view.autofill.IAutoFillManager]	90	content: [android.content.IContentService]
19	imms: [com.android.internal.telephony.IMms]	91	account: [android.accounts.IAccountManager]
20	media.camera.proxy: [android.hardware.ICameraServiceProxy]	92	DirEncryptService: [IDirEncryptService]
21	media_projection: [android.media.projection.IMediaProjectionManager]	93	SatsService: [com.samsung.android.service.sats.ISatsService]
22	launcherapps: [android.content.pm.ILauncherApps]	94	overlay: [android.content.om.IOverlayManager]
23	shortcut: [android.content.pm.IShortcutService]	95	EngineeringModeService: [com.samsung.android.service.EngineeringMode.IEngineeringModeService]
24	media_router: [android.media.IMediaRouterService]	96	VaultKeeperService: [com.samsung.android.service.vaultkeeper.IVaultKeeperService]
25	media_session: [android.media.session.ISessionManager]	97	ReactiveService: [com.samsung.android.service.reactive.IReactiveService]
26	restrictions: [android.content.IRestrictionsManager]	98	telephony.registry: [com.android.internal.telephony.ITelephonyRegistry]
27	companiondevice: [android.companion.ICompanionDeviceManager]	99	scheduling_policy: [android.os.ISchedulingPolicyService]
28	print: [android.print.IPrintManager]	100	sec_key_att_app_id_provider: [android.security.keymaster.IKeyAttestationApplicationIdProvider]
29	graphicsstats: [android.view.IGraphicsStats]	101	webviewupdate: [android.webkit.IWebViewUpdateService]
30	dreams: [android.service.dreams.IDreamManager]	102	usagestats: [android.app.usage.IUsageStatsManager]
31	commontime_management: []	103	battery: []
32	network_time_update_service: []	104	sensorservice: [android.gui.SensorServer]
33	diskstats: []	105	dropbox: [com.android.internal.os.IDropBoxManagerService]
34	voiceinteraction: [com.android.internal.app.IVoiceInteractionManagerService]	106	processinfo: [android.os.IProcessInfoService]
35	appwidget: [com.android.internal.appwidget.IAppWidgetService]	107	permission: [android.os.IPermissionController]
36	backup: [android.app.backup.IBackupManager]	108	cpuinfo: []
37	trust: [android.app.trust.ITrustManager]	109	dbinfo: []
38	soundtrigger: [com.android.internal.app.ISoundTriggerService]	110	gfxinfo: []
39	jobscheduler: [android.app.job.IJobScheduler]	111	meminfo: []
40	hardware_properties: [android.os.IHardwarePropertiesManager]	112	procstats: [com.android.internal.app.procstats.IProcessStats]
41	serial: [android.hardware.ISerialManager]	113	activity: [android.app.IActivityManager]
42	usb: [android.hardware.usb.IUsbManager]	114	user: [android.os.IUserManager]
43	DockObserver: []	115	otadexopt: [android.content.pm.IOtaDexopt]
44	audio: [android.media.IAudioService]	116	package_native: [android.content.pm.IPackageManagerNative]
45	wallpaper: [android.app.IWallpaperManager]	117	package: [android.content.pm.IPackageManager]
46	search: [android.app.ISearchManager]	118	media.camera: [android.hardware.ICameraService]
47	country_detector: [android.location.ICountryDetector]	119	display: [android.hardware.display.IDisplayManager]
48	location: [android.location.ILocationManager]	120	recovery: [android.os.IRecoverySystem]
49	devicestoragemonitor: []	121	power: [android.os.IPowerManager]
50	notification: [android.app.INotificationManager]	122	appops: [com.android.internal.app.IAppOpsService]
51	updatelock: [android.os.IUpdateLock]	123	batterystats: [com.android.internal.app.IBatteryStats]
52	knoxguard_service: [com.samsung.android.knoxguard.IKnoxGuardManager]	124	device_identifiers: [android.os.IDeviceIdentifiersPolicyService]

53	servicediscovery: [android.net.nsd.INsdManager]	125	media.sound_trigger_hw: [android.hardware.ISoundTriggerHwService]
54	connectivity: [android.net.IConnectivityManager]	126	media.audio_policy: [android.media.IAudioPolicyService]
55	ethernet: [android.net.IEthernetManager]	127	netd: []
56	wifip2p: [android.net.wifi.p2p.IWifiP2pManager]	128	media.audio_flinger: [android.media.IAudioFlinger]
57	rttmanager: [android.net.wifi.IRttManager]	129	media.extractor: [android.media.IMediaExtractorService]
58	wifiscanner: [android.net.wifi.IWifiScanner]	130	media.resource_manager: [android.media.IResourceManagerService]
59	wifi: [android.net.wifi.IWifiManager]	131	media.player: [android.media.IMediaPlayerService]
60	netpolicy: [android.net.INetworkPolicyManager]	132	storaged: [Storaged]
61	netstats: [android.net.INetworkStatsService]	133	media.metrics: [android.media.IMediaAnalyticsService]
62	network_score: [android.net.INetworkScoreService]	134	android.security.keystore: [android.security.IKeystoreService]
63	textservices: [com.android.internal.textservice.ITextServicesManager]	135	wificond: []
64	network_management: [android.os.INetworkManagementService]	136	android.service.gatekeeper.IGateKeeperService: []
65	enterprise_policy: [com.samsung.android.knox.IEnterpriseDeviceManager]	137	installld: []
66	edm_proxy: [android.sec.enterprise.IEDMProxy]	138	lextSDUFsServiceVold.unionFSStackServiceVold: []
67	clipboard: [android.content.IClipboard]	139	media.drm: [android.media.IMediaDrmService]
68	statusbar: [com.android.internal.statusbar.IStatusBarService]	140	gpu: [android.ui.IGpuService]
69	device_policy: [android.app.admin.IDevicePolicyManager]	141	SurfaceFlinger: [android.ui.ISurfaceComposer]
70	deviceidle: [android.os.IDeviceIdleController]	142	batteryproperties: [android.os.IBatteryPropertiesRegistrar]
71	oem_lock: [android.service.oemlock.IOemLockService]	143	thermalservice: [android.os.IThermalService]

Third Party Applications

Number of Third Party Applications installed on Device: 22

3rd Party Applications installed on Device-Samsung

com.amazon.dee.app	com.acr.androiddownloadmanager
com.hdwallpaper.wallpaper	com.mgs.obcbank
com.yaantraportal.app	org.edx.mobile
com.google.android.apps.tachyon	com.google.android.apps.nbu.paisa.user
com.google.android.apps.docs	com.hdw.blackwallpapers
net.one97.paytm	com.google.android.apps.books
com.fss.mobilepay.obc	com.unacademyapp
com.ovelin.guitartuna	in.swiggy.android
net.rention.mind.skillz	com.kiloo.subwaysurf
com.google.android.apps.photos	com.google.android.play.games
com.spotify.music	

Section B. Malware Report

Malware Report of SAMSUNG Device

DEVICENAME	APPNAME	SHA256	ENGINE1	ENGINE2	ENGINE3	ENGINE4	ENGINE5	ENGINE6	OVERALL
SAMSUNG	USBSettings.apk	78a7867ce2138affa1ea048f2269235e7ccd85d2c826e574929d49a4591067b6	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	68.apk	90bd835322d43ea168d17de2c2b9673d122132dd8fb8b8abd69ddf912c1e1531	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	43.apk	ab3d4257f9bf7f6e4ad46b6f310aa19441cc5a05b65ae924733636bc369c0464	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	63.apk	06064ae06df90687bb394f7c2e277c2df1901cf0151ef0688940e1c6b2799a00	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	128.apk	63057e11c73f1acc8f067f49e138dfae51f002425094e25396959d29edccd4f8	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	WebManual.apk	2965709f24bc893d7ee6be11500917bf7904839e15bc25709dfcdf18dca803c3	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	ConfigUpdater.apk	132524cecec8f980d4feaae5ea30897b220c006f172f357bb5f3aba76fbb9b685	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	Telecom.apk	d51518c250274de40af3f70e5ec061c08f64bfaeae2c0453c22ddac39f4b74fe	SAFE	SAFE	SAFE	MALWARE	SAFE	SAFE	MALWARE
SAMSUNG	SharedStorageBackup.apk	c7bb782161ad7083397d5da3ad75561f60b296cfbabd6de9deb3e1abd3ae395f	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	SafetyInformation.apk	ff6d4b2715235ef946d6f444d738ff8cdeec7f11df9d7258ed2734234831ad58	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	CtsShimPrebuilt.apk	56a6e3cba1ebb0c6e1257e3d15f715b39174bfc259ece918cfb353dc7b6d208c	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	124.apk	e2386b7a49abb806f05f2a54149f8e7649c282b7a13856b061e3ecb58227a0c4	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	BluetoothMidiService.apk	897c3dc239a54995590ab6aff2306107227b96bea4e9ff7596debb58a5c4abfe	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	PartnerBookmarksProvider.apk	350b859043e61e9640f82cf69f8cb4ca35390f1d020b31f5d053866d33bea74d	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	120.apk	64b2a6c43b81af8e556a6c1f1af5972a70d372e7adb9139a021a91980dd97c65	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	SamsungMembersWeb.apk	f0b91f8ef37cbafbf153dfedfcfdc0705062e0c748ea952dab45475ac0a2d95	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	sveservice.apk	4fc99a2f75f4117b996690f329b31ee3f1cd855246971384e05d0bc3edb8e176	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	InputDevices.apk	5196fc4bbd0a4373e409ba9652880cc125f4e3c3877384331b6be07f7a6e233a	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	BasicDreams.apk	0008c94cad3026428e5e5f98893da7399ef86efc5a758b35a8822269cb062de0	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	GoogleExtShared.apk	f595eee40a8981913cec9d4b572604e855c6925ceeBB12501ccf161c03525d88	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	18.apk	bdb51e1ff28bff2c5898c99813921b9dcfc902947b912a7669a1fb807db47398	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	MmsService.apk	0dffe14452ec67e2bb22d6bf13412551fc82af36cfddea557b68d8f2a5e102d6	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	CompanionDeviceManager.apk	2b10b23bde48bab09e86a10c1d261d8e89f2b721f6d2b498860d6f6f93dc7d57	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	GoogleFeedback.apk	69042bdf784e82afb8a052a57a3d1310a7f41c209e126189ebb479262da4cb3	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	33.apk	4981a925a02c15b1fffd686a8f0ffab125c1d1908d6194f5a66abe93a04361a	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	CtsShimPrivPrebuilt.apk	1b930afd81f765a3366f21e57cfcfdefc867fda93e859b136aeef27ecfd9cb0c	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	MtpDocumentsProvider.apk	3f86ea3a471060c16046437919ac55d691935de70f9c7fae23113ae0699880c9	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	BlockedNumberProvider.apk	bb6f20607f6fc0645c22b904a5efbf3ce8b0defbe434f29433850abed411ec57	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	EmergencyProvider.apk	d605d4edb336c36dd0f6c69e73da143fab2ac02917bb341d4ab8a96793e45471	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	CarrierConfig.apk	52a3fc0e06a3dae5e56f761d13c5a68fc0d5c5dc982aa2aff396c8280cd8ba06	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	EasterEgg.apk	93e5438ad4dcca33401e463073da23a49c0dc5a3ebd241f7f5e09a7adae88b24	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	CaptivePortalLogin.apk	b07497ff08434c2e2f75824cbeefee3f9722605f6b5e84d753fc146f200ec8c3	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	SVCAgent.apk	24ed027c64077fb0340f03153a314441e5fbe5301465b48c4b43fcdeca49d2ac	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	CertInstaller.apk	2133393ec33561c7626f2a793b3c2282fcefca44a05c8d1904785d5c97d4a71b6	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	DownloadProviderUi.apk	a95de6a4921263571aa80a0f6c8ce4b627a0bed9b5d58cd07ad656bba89d9592	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	StatementService.apk	82c225e98635a4a4802fc4db87c79a26265e6da99e8841de4bdb7e3ec418d275	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	GoogleCalendarSyncAdapter.apk	226cfc3c642344e526ad549d39f239f81362e023282cd04b042a6165cf80a78c	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	UserDictionaryProvider.apk	bd99056695cba71b752895e0cb6f386129212e71508045366dadd0f85bce0f6a	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	ChromeCustomizations.apk	2d8ca57ef92c138a5746f31474b13df862573896cb4e7ebc4d1d4c134ae4433b	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	TetheringAutomation.apk	f8cc6e023ea00310a236db5638c9a0b6f5a93254ab9191fc9b34308dabcc1da2	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	BookmarkProvider.apk	c0fc4e99ad48f3a0fa31d4f4ef370c5b324ae6cfe5164acc882b2da17c8f5a5f	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	WebViewStub.apk	52ab35b1954f79153146a081ce16100acd49838092b86c0666b91e2261578a24	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	GoogleBackupTransport.apk	17cce998da6b971f7505bff6d3a22b75840841c7cb04f46f4b4c087965a238bf	MALWARE	MALWARE	SAFE	SAFE	SAFE	SAFE	MALWARE
SAMSUNG	StorageManager.apk	d5dcbbfdfbcfde899040f2cb188e00ef69e6ce797dfdbbbf10ffc4bd277522a3	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	WallpaperBackup.apk	ffe5a7a80556955f9eff079bde0df41dba9c0672a714ab557811f3adc972f07f	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	ManagedProvisioning.apk	9dacc57b070249cb04ddcd76488543e64bc332527aa134df8c410ca4820d4ab2	SAFE	SAFE	SAFE	MALWARE	SAFE	SAFE	MALWARE
SAMSUNG	Personalization.apk	e05d50b06c5344cb860332e24a6b88ebf8ad0cb80bac85206fdb0409a0fc2478	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	SettingsProvider.apk	923affa03583c5c80e0cf7c414f6fc8886a2042935f9c3cc603ebdbf016f7da5	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	140.apk	75fe206f737e736c94a763829fd08142c3fe8c6034a4fd4d20bfdfdd11fd904	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	SmartSwitchAssistant.apk	61ca44d8fa3a1580f76ea878e0c721199369ed522e80b5466344f56b098a5562	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	HTMLViewer.apk	f7cba5a103fedf5e963899a364324643a68daa84e5fe0c0e62eb10b96100051b	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	WallpaperCropper.apk	fa05899bad950340c97f75e58fb8b3e8e7f8268d93527a924f4e10178e845310	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	CallLogBackup.apk	3c28da901b755766ce3d59e1a0c4e62756968d44b7fbc968b9369e1f3a2818ca	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	SOAgent.apk	2be74dd3df03526c7bb40c143609d17fb6d5a892cd263380a5a43a16aab76a65	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	KeyChain.apk	af9a27603c41a572bfaa20a1e3152eb48f9d7ed2fbb178b16e347d0bb8d8ef86	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE
SAMSUNG	SamsungTimeZoneUpdater.apk	e75acdd5bd2adad8779d0e88b53c5e9657835f8c054e8c36d5ef6927b6ba8f5c	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE	SAFE

Section C. CVE Report

CVE Report of Samsung 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_FormFilter::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 craftedtext.
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::nonBoundaryShadowTreeRootNode 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 ofintent: 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 videostream.
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-2014-5821	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.
	The Guitar Tuner Free - GuitarTuna (aka com.ovelin.guitartuna) application 2.4.5 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
Facebook Lite	Varies with device
Google Drive	Varies with device
Google Photos	Varies with device
Google Play Games	Varies with device
Skillz-Logic Brain Games	5.1.6

Suggestion for Deletion of Apps

Appilication name
Telecom.
GoogleBackupTransport.
ManagedProvisioning.
BackupRestoreConfirmation.