学术论文

JGRE：安卓系统JNI全局引用耗尽漏洞分析
JGRE: An Analysis of JNI Global Reference Exhaustion Vulnerabilities in Android

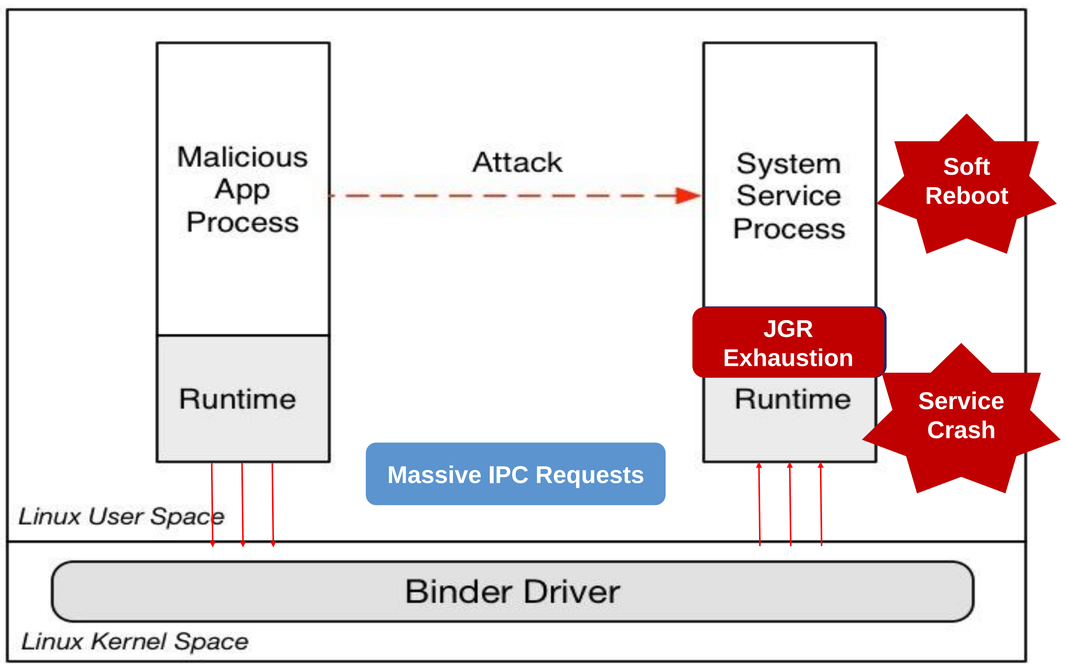
谷雅聪*, Kun Sun#, 苏璞睿*†, 李琦‡, 路晔绵*,应凌云*†, 冯登国*

*Institute of Software, Chinese Academy of Sciences
#George Mason University †University of Chinese Academy of Sciences
‡Graduate School at Shenzhen, Tsinghua University

The 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2017), Denver, CO, United States, 2017, pp. 427-438.

（应凌云，lingyun@iscas.ac.cn）

- JNI Global Reference是Android系统的重要系统资源，论文对Android系统的JNI Global Reference使用问题进行了深入研究，发现了大量未知的安全漏洞，并在此基础上提出了一个可以有效检测此类漏洞攻击的通用防御框架。
- 该项研究共发现了Android系统的32个系统服务（占全部104个系统服务的30.8%）中存在的54个安全漏洞，其中，针对19个系统服务中32安全漏洞的攻击不需要任何权限。
- 此外，还发现了2个内嵌应用软件存在的3个安全漏洞、以及2个存在漏洞的第三方应用软件。
- 相关漏洞可以导致应用软件退出、系统服务崩溃、操作系统重启等问题，影响包括7.0版在内的各个版本Android系统，对智能手机、智能手表、互联网电视等众多使用Android系统的智能终端设备造成严重安全威胁。
- Google已经确认了该项研究工作发现的所有漏洞，并在相关漏洞安全更新中对该论文研究工作表示了感谢。



UNPROTECTED VULNERABLE IPC INTERFACES

Service Name	Vulnerable IPC Interface	Required Permission (Protection Level) in AOSP 6.0.1
location	addGpsStatusListener	ACCESS_FINE_LOCATION (dangerous)
sip	open3	USE_SIP (dangerous)
	createSession	USE_SIP (dangerous)
midi	registerListener	-
	openDevice	-
	openBluetoothDevice	-
	registerDeviceServer	-
content	registerContentObserver	-
	addStatusChangeListener	-
mount	registerListener	-
appops	startWatchingMode	-
	getToken	-
bluetooth_manager	registerAdapter	-
	registerStateChangeCallback	BLUETOOTH (normal)
	bindBluetoothProfileService	-
	bindBluetoothProfileService	-
audio	registerRemoteController	-
	startWatchingRoutes	-
country_detector	addCountryListener	-
power	acquireWakeLock	WAKE_LOCK (normal)
input_method	addClient	-
accessibility	addAccessibilityInteractionConnection	-
print	print	-
	addPrintJobStateChangeListener	-
	createPrinterDiscoverySession	-
package	getPackageSizeInfo	GET_PACKAGE_SIZE (normal)
telephony.registry	addOnSubscriptionsChangedListener	READ_PHONE_STATE (dangerous)
	listen	READ_PHONE_STATE (dangerous)
	listenForSubscriber	READ_PHONE_STATE (dangerous)
media_session	registerCallbackListener	-
	createSession	-
media_router	registerClientAsUser	-
media_projection	registerCallback	-
input	vibrate	-
window	watchRotation	-
wallpaper	getWallpaper	-
fingerprint	addLockoutResetCallback	-
textservices	getSpellCheckerService	-
network_management	registerNetworkActivityListener	CHANGE_NETWORK_STATE (normal)
connectivity	requestNetwork	CHANGE_NETWORK_STATE (normal)
	listenForNetwork	ACCESS_NETWORK_STATE (normal)
activity	registerTaskStackListener	-
	registerReceiver	-
	bindService	-