

安卓安全补丁

安卓安全补丁.....	1
1. 安卓安全补丁起源:	1
2. Android 更新月度说明.....	3
3. 案件讲解, 怎样搜寻漏洞, 并获得解决方案。.....	4
4. 认证策略和输出文档.....	6

1. 安卓安全补丁起源:

一则新闻标题: 向 OEM 推安卓补丁 谷歌旨在修复安全漏洞, 2014-04-18 消息

谷歌向 OEM 推动一个 Android 安全补丁, 旨在修复允许某些恶意应用引导用户进入钓鱼网站窃取用户信息的安全漏洞。这个漏洞最先被网络安全公司 FireEye 发现, 会启动第三方应用利用安卓权限“com.android.launcher.permission.READ_SETTINGS”和“com.android.launcher.permission.WRITE_SETTINGS”, 改变安卓启动器的图标和默认设置。这个漏洞影响所有版本的安卓系统, 包括 Android 4.4.2。

有趣的是, 这两项权限会被谷歌视为“正常”, 这意味着它们可以自动提供给无需特定授予权限的应用和用户。此外, 也不会有提醒告知已获得这些权限, 这便让违规者有机可乘。这个恶意应用更改某一图标吸引用户注意并点击, 这便会将用户带到钓鱼网站从而获取用户隐私信息。

FireEye 在 2013 年 10 月份发现了这个漏洞和利用这个漏洞的应用。二月份, 谷歌透露准备发布补丁, 近期才向合作商推送。

[谷歌 Android 安全 Android 系统](#)自 2015 年 12 月份开始, Google 公司要求所有基于 Android 的新版系统中加入一项说明, 补丁程序级别; 这项说明是关于内部一些安全问题的修复内容; 这个新增项对于用户使用来说并不会带来什么影响。

安卓系统安全补丁什么时候更新一次, 谷歌一直致力于维护安卓系统的最新安全性, 但是由于谷歌安卓系统的严重碎片化的问题, 谷歌的频繁安全补丁更新并没有得到太多手机厂商的支持。现在联想旗下的摩托罗拉也退出了这一月度安全更

新行列，看样子谷歌的话语权进一步减弱了。

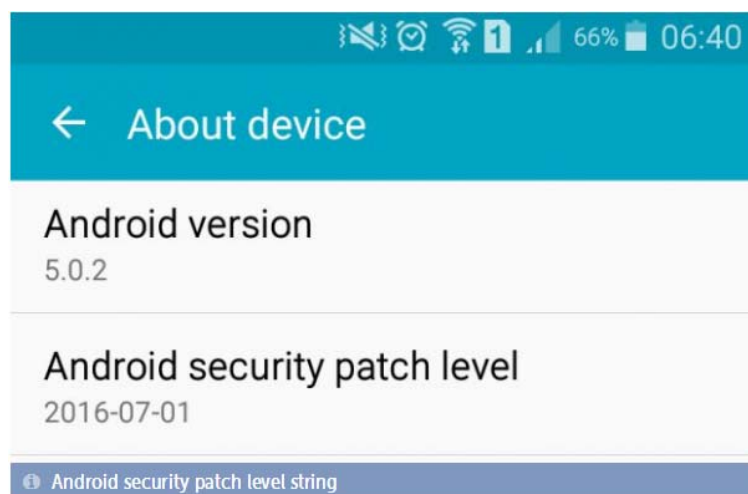
谷歌定期会面向安卓设备推送安全补丁，一般频度是按月。

之前因采用原生系统而与 Nexus 一样勤勉获得更新的 Motor 却悄然宣布，**2016 年的新品比如 Motor ZIG4 将不再同步谷歌的节奏进行常规性的月度安全更新。**

Motor 此前都会将安全补丁打包到系统稳定更新中，但现在他们发现这样做越来越难。

此举意味着，从 2016 年开始，在谷歌发布月度安全补丁的时候，Motor 的新机将不会保持一致的更新步伐，而是和自己既定的系统稳定更新日程一致，言外之意就是滞后许多了。

目前，严格参与谷歌月度安全更新的厂商有黑莓、三星和 LG，亲儿子 Nexus 自不用说。



2016-09-01 security patch level—Vulnerability summary

Issue	CVE	Severity	Affects Nexus?
Remote code execution vulnerability in LibUtils	CVE-2016-3861	Critical	Yes
Remote code execution vulnerability in Mediaserver	CVE-2016-3862	Critical	Yes
Remote code execution vulnerability in MediaMuxer	CVE-2016-3863	High	Yes

小米手机保持每个月推送一个稳定版本，包含了 Google 官方的补丁。

补充旧闻：

标题： 安卓安全补丁发布： 修复 23 个系统漏洞

2015-11-03 来源： 下载之家 作者： 石头

导读：Google 已启动每月为 Android 推送一次安全补丁的计划了，现在，11 月份的 Android 安全补丁发布了。谷歌在 11 月 3 日推出了最新的 Android 安全补丁，这个补丁将会为 Nexus 设备推送。这是一个非常关键的补丁，修复多达 23 个漏洞，Nexus 客户可留意一下近日是否有系统更新。

早先，HTC 也吐槽谷歌打补丁有些过于频繁严格，而悄悄退出了支持行列。按照谷歌的说法，它们是 Android 内核的开发者的，有着系统安全最高的话语和指挥权，每月的安全补丁至关重要。

Google 已启动每月为推送一次安全补丁的计划了，现在，11 月份的 Android 安全补丁发布了。谷歌在 11 月 3 日推出了最新的 Android 安全补丁，这个补丁将会为 Nexus 设备推送。这是一个非常关键的补丁，修复多达 23 个漏洞，Nexus 客户可留意一下近日是否有系统更新。

据了解，Google 这次的补丁修复了 23 个漏洞，其中 2 个为高危漏洞，黑客可利用这两个漏洞在客户收发邮件、浏览网页、阅读短信处理媒体文件时进行远程控制。Google 强烈建议客户跟进这次升级，以免受到黑客侵扰。

这次 Google 的 Android 安全补丁将会向 Nexus 设备推送，具体的型号则是 Nexus 6P、Nexus 5X、Nexus 9、Nexus 7、Nexus 6、Nexus 5 以及 Nexus Player。Nexus 设备的 OTA 推送会在 48 小时内到来，如果你等不及推送，也能够自行下载系统镜像自行刷入。除了 Nexus 设备外，三星以及 LG 也称会跟进这些安全补丁，希望有更多的厂商为客户提供补丁推送吧。

2.Android 更新月度说明

Android 更新月度说明(2017-05-01)：（需翻墙）

<https://source.android.com/security/bulletin/2017-05-01>

3. 案件讲解，怎样搜寻漏洞，并获得解决方案。

从以下网站搜索公开漏洞：

Common Vulnerabilities and Exposures

<http://cve.mitre.org/cve/cve.html>

或者

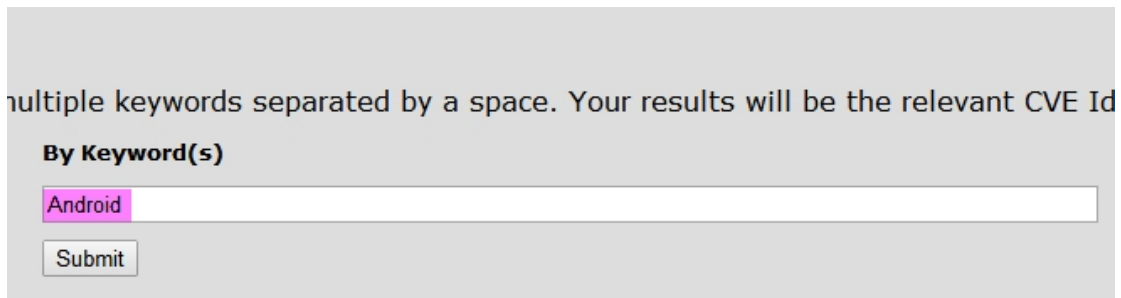
Computer Security Resource Center

National Vulnerability Database

<https://nvd.nist.gov/vuln/search>

在这两个网站搜索框，输入的关键字可以是：**Android** 或者 **linux** 或者 **openssl**，**Android**、**linux**、**openssl** 在认证前必须打上对应版本上，涉及安全的已经公开的所有漏洞补丁。

现在以 CVE 网站 <http://cve.mitre.org/cve/cve.html>，关键词以 **Android** 为例：



multiple keywords separated by a space. Your results will be the relevant CVE Id

By Keyword(s)

Android

Submit

搜索到一系列 Android 漏洞，以下以编号 **CVE-2017-0553** 为例，查找解决方案。

CVE-2017-0555	An information disclosure vulnerability in libavc in Mediaserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access data without permission. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33551775.
CVE-2017-0554	An elevation of privilege vulnerability in the Telephony component could enable a local malicious application to access capabilities outside of its permission levels. This issue is rated as Moderate because it could be used to gain access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33815946.
CVE-2017-0553	An elevation of privilege vulnerability in libnl could enable a local malicious application to execute arbitrary code within the context of the Wi-Fi service. This issue is rated as Moderate because it first requires compromising a privileged process and is mitigated by current platform configurations. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32342065.
CVE-2017-0552	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34097915.
CVE-2017-0551	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34097231.
CVE-2017-0550	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33933140.

点击**进入**箭头处会进入 CVE 漏洞曝光网站：

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0553>

CVE-ID

CVE-2017-0553
[Learn more at National Vulnerability Database \(NVD\)](#)

- Severity Rating
- Fix Information
- Vulnerable Software Versions
- SCAP Mappings

Description

An elevation of privilege vulnerability in libnl could enable a local malicious application to execute arbitrary code within the privileged process and is mitigated by current platform configurations. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32342065.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be exhaustive.

- [CONFIRM:https://source.android.com/security/bulletin/2017-04-01](https://source.android.com/security/bulletin/2017-04-01)
- BID:97340
- URL:http://www.securityfocus.com/bid/97340

获取更多描述

点击 **获取更多描述** 箭头处会进入 NVD 漏洞更多描述

<https://nvd.nist.gov/vuln/detail/CVE-2017-0553>

Vulnerabilities > Detail

CVE-2017-0553
Detail

Current Description

An elevation of privilege vulnerability in libnl could enable a local malicious application to execute arbitrary code within the context of the Wi-Fi service. This issue is rated as Moderate because it first requires compromising a privileged process and is mitigated by current platform configurations. Product: **Android Versions:** 5.0.2, 5.1.1, 6.0, **6.0.1**, 7.0, 7.1.1. Android ID: A-32342065.

Source: MITRE Last Modified: 04/07/2017 [View Analysis Description](#)

Quick Info

CVE Dictionary Entry: **CVE-2017-0553**
Original release date: 04/07/2017
Last revised: 04/12/2017
Source: US-CERT/NIST

Impact

CVSS Severity (version 3.0):
CVSS v3 Base Score: 7.0 High
Vector: **CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:A/H (legend)**
Impact Score: 5.9
Exploitability Score: 1.0

CVSS Version 3 Metrics:
Attack Vector (AV): Local
Attack Complexity (AC): High
Privileges Required (PR): None
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Severity (version 2.0):
CVSS v2 Base Score: 7.6 HIGH
Vector: **(AV:N/AC:H/Au:N/C:C/I:A/C)** (legend)
Impact Subscore: 10.0
Exploitability Subscore: 4.9

CVSS Version 2 Metrics:
Access Vector: Network exploitable - Victim must voluntarily interact with attack mechanism
Access Complexity: High
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

References to Advisories, Solutions, and Tools

解决方案

点击 **解决方案** 箭头处，会进入解决方案代码下载网站(2017-04-01)：（需翻墙）

<https://source.android.com/security/bulletin/2017-04-01>

在网站查找 **CVE-2017-0560** References **A-30681079**

Information disclosure vulnerability in Factory Reset

An information disclosure vulnerability in the factory reset process could enable a local malicious attacker to access data from the previous owner. This issue is rated as Moderate due to the possibility of bypassing device protection.

CVE	References	Severity	Updated Google devices	Updated AOSP versions	Date reported
CVE-2017-0560	A-30681079	Moderate	All	4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1	Google internal

解决方案

点击 **解决方案** 箭头处，会进入 A-30681079 References 代码链接：

<https://android.googlesource.com/platform/frameworks/base/+efdec8f5688ce6b0a287eddb6d5dad93ffa0e1ee%5E%21/#F0>

漏洞补丁的片段:

```
@@ -4750,7 +4750,7 @@      }      }  
- private void wipeDataLocked(boolean wipeExtRequested, String reason) {  
+ private void wipeDataNoLock(boolean wipeExtRequested, String reason) {  
if (wipeExtRequested) {  
StorageManager sm = (StorageManager) mContext.getSystemService(  
Context.STORAGE_SERVICE);
```

4. 认证策略和输出文档

认证时要求支持远程固件更新（OTA 更新），会对安卓安全补丁的版本更新周期有要求,一般是 3 个月左右。我们需要对 Z5 Android6.0 所涉及的漏洞（Android 安全补丁主要针对 Android 框架, 另外还有 Linux 内核和 Openssl 开源加密算法库的安全漏洞）进行评估, 修复, 记录, 测试, 审核, 并保存修复 Patch 以供认证机构审核。

主要涉及的文档有:

Vulnerability Assessment Document 详细说明漏洞的搜寻, 补丁, 维护策略文档。

Vulnerability Assessment Approval Form.xlsx 打完漏洞评估审批表格。

Vulnerability Assessment Record.xlsx 漏洞评估记录文档。

Vulnerability Disclosure Form.xlsx 漏洞披露表格, 说明已经打过多少漏洞的 Patch。

Vulnerability Testing Approval Form.xlsx 漏洞测试结果审批表格。

Vulnerability Testing Record.xlsx 漏洞测试记录。

Vulnerability Assessment Record 格式如下, 来源于潘龙提供资料模板。

Note: On the 1st of each month, the developer needs to check vulnerability in the website: 1 http://cve.mitre.org/about/index.htm with the keyword "openssl" "linux" and "android", and generate this record. (The vulnerabilities which do not affect the security of the device will not be recorded).					
Developer: 2 Vulnerability Scanning Method: Review the information in the public domain: http://cve.mitre.org/about/index.htm System Version: Date:					
3	Vulnerability Type	Vulnerability Identification	Criticality	Vulnerability Description or Effects to Device	Mitigation Method
4	OpenSSL	CVE-2013-4353	Medium	The ssl3_take_mac function in ssl/s3_both.c in OpenSSL 1.0.1 before 1.0.1f allows remote TLS servers to cause a denial of service (NULL pointer dereference and application crash) via a crafted Next Protocol Negotiation record in a TLS handshake.	Add patch
5					
6					
7					
8					
9					
10					
11					