

信息安全漏洞周报

2015 年 04 月 20 日-2015 年 04 月 26 日

2015 年第 17 期

本周漏洞基本情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 194 个，其中高危漏洞 59 个、中危漏洞 111 个、低危漏洞 24 个。上述漏洞中，可利用来实施远程攻击的漏洞有 174 个。本周收录的漏洞中，已有 173 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。其中互联网上出现“Cisco Unified MeetingPlace Custom Prompts 任意文件上传漏洞”、“D-Link DIR-890L 命令执行漏洞”等零日漏洞，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 6 家成员单位、合作伙伴及个人报送了本周收录的全部 194 个漏洞。报送情况如表 1 所示。其中，天融信、启明星辰、安天实验室、绿盟科技等单位报送数量较多。此外，CNCERT 各分中心、上海天泰网络技术有限公司、乌云、漏洞盒子、High-Tech Bridge Security Research Lab 及白帽子向 CNVD 提交了 280 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
天融信	187	0
安天实验室	134	0
绿盟科技	104	0
启明星辰	87	0
恒安嘉新	50	0
知道创宇	10	0

乌云	227	227
漏洞盒子	17	17
High-Tech Bridge Security Research Lab	1	1
上海天泰网络技术有 限公司	1	1
CNCERT 山西分中心	13	13
CNCERT 陕西分中心	4	4
CNCERT 江西分中心	4	4
CNCERT 福建分中心	1	1
CNCERT 宁夏分中心	1	1
个人	11	11
报送总计	852	280
录入总计	194（去重）	280

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、Drupal、Google 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Oracle	72	37%
2	Drupal	19	10%
3	Google	17	9%
4	Adobe	11	6%
5	Cisco	10	5%
6	WordPress	6	3%
7	Apple	4	2%
8	OrangeHRM	4	2%
9	Apache	2	1%
10	其他	49	25%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周, CNVD 收录了 194 个漏洞。其中应用程序漏洞 124 个, WEB 应用漏洞 32 个, 数据库漏洞 21 个, 操作系统漏洞 10 个, 网络设备漏洞 5 个, 安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	124
WEB 应用漏洞	32
数据库漏洞	21
操作系统漏洞	10
网络设备漏洞	5
安全产品漏洞	2

表 3 漏洞按影响类型统计表

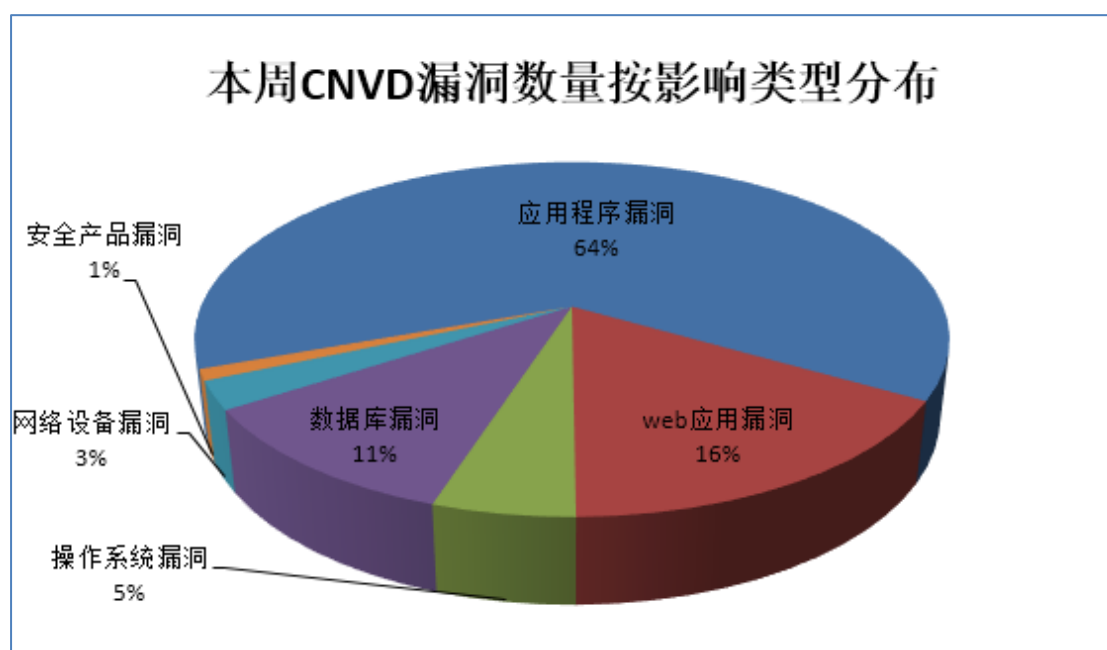


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周, CNVD 收录了 32 个电信行业漏洞, 2 个移动互联网行业漏洞 (如下图表所示)。其中, “Oracle Database Server VM 组件存在未明漏洞、Oracle Fusion Middleware Access Manager 组件存在未明漏洞、IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞、Cisco IOS XR Software 拒绝服务漏洞 (CNVD-2015-02658)、Cisco Secure Desktop (CSD)任意命令执行漏洞” 的综合评级均为 “高危”。相关厂商已经发布了上述漏洞的修补程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
----	------	------	------	-------

电信	CNVD-2015-02520	Oracle Database Server 存在远程漏洞 (CNVD-2015-02520)	中	是
电信	CNVD-2015-02521	Oracle Database Server 存在远程漏洞 (CNVD-2015-02521)	中	是
电信	CNVD-2015-02522	Oracle Database Server 存在远程漏洞 (CNVD-2015-02522)	中	是
电信	CNVD-2015-02537	Oracle Fusion Middleware WebLogic Server 组件存在未明漏洞	中	是
电信	CNVD-2015-02539	Oracle Fusion Middleware WebCenter Portal 组件存在未明漏洞 (CNVD-2015-02539)	中	是
电信	CNVD-2015-02538	Oracle Fusion Middleware OpenSSO 组件存在未明漏洞	低	是
电信	CNVD-2015-02540	Oracle Fusion Middleware WebCenter Portal 组件存在未明漏洞 (CNVD-2015-02540)	中	是
电信	CNVD-2015-02577	Oracle Database Server VM 组件存在未明漏洞	高	是
电信	CNVD-2015-02576	Oracle Fusion Middleware Access Manager 组件存在未明漏洞	高	是
电信	CNVD-2015-02565	Oracle MySQL Server Server:Optimizer 子组件存在未明漏洞	中	是
电信	CNVD-2015-02566	Oracle MySQL Server Server:Optimizer 子组件存在未明漏洞 (CNVD-2015-02566)	中	是
电信	CNVD-2015-02567	Oracle MySQL Server Server:Partition 子组件存在未明漏洞	中	是
电信	CNVD-2015-02568	Oracle MySQL Server Server:DDL 子组件存在未明漏洞	低	是
电信	CNVD-2015-02569	Oracle MySQL Server Server:Federated 子组件存在未明漏洞	低	是
电信	CNVD-2015-02570	Oracle MySQL Server Server:InnoDB 子组件存在未明漏洞	低	是
电信	CNVD-2015-02571	Oracle MySQL Server Server:Memcached 子组件存在未明漏洞	低	是
电信	CNVD-2015-02572	Oracle MySQL Server Server:Security:Privileges 子组件存在未明漏洞	低	是
电信	CNVD-2015-02573	Oracle MySQL Server Server:Partition 拒绝服务漏洞	中	是
电信	CNVD-2015-02574	Oracle MySQL Server Server:DML 子组件存在未明漏洞	中	是
电信	CNVD-2015-02564	Oracle MySQL Server Server:SP 子组件存在未明漏洞	低	是
电信	CNVD-2015-02563	Oracle MySQL Server Server:Replicatio	低	是

		n 子组件存在未明漏洞		
电信	CNVD-2015-02562	Oracle MySQL Server Server:InnoDB:D ML 拒绝服务漏洞	中	是
电信	CNVD-2015-02561	Oracle MySQL Server Server:XA 子组 件拒绝服务漏洞	中	是
电信	CNVD-2015-02560	Oracle MySQL Server Server:Security:E ncryption 拒绝服务漏洞	中	是
电信	CNVD-2015-02590	Oracle Fusion Middleware WebLogic S erver 组件存在未明漏洞（CNVD-2015-0 2590）	中	是
电信	CNVD-2015-02589	Oracle Fusion Middleware Outside In Technology 组件拒绝服务漏洞	低	是
电信	CNVD-2015-02635	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞	高	是
电信	CNVD-2015-02640	Oracle MySQL Server Connector/J 子组 件存在未明漏洞	中	是
电信	CNVD-2015-02643	D-Link DIR-890L 命令执行漏洞	高	否
电信	CNVD-2015-02658	Cisco IOS XR Software 拒绝服务漏洞 （CNVD-2015-02658）	高	是
电信	CNVD-2015-02694	Oracle Fusion Middleware Outside In Technology 组件拒绝服务漏洞	低	是
电信	CNVD-2015-02716	Cisco Secure Desktop (CSD)任意命令 执行漏洞	高	是
移动互联网	CNVD-2015-02534	USAA Mobile Banking 应用程序存在未 明漏洞	低	是
移动互联网	CNVD-2015-02535	LIXIL Corporation My SATIS Genius Toilet 应用程序存在未明漏洞	低	否

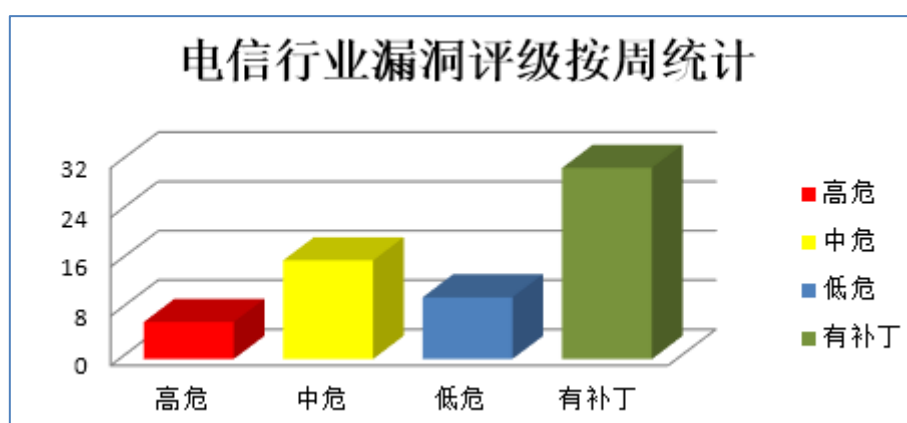


图 1 电信行业漏洞统计

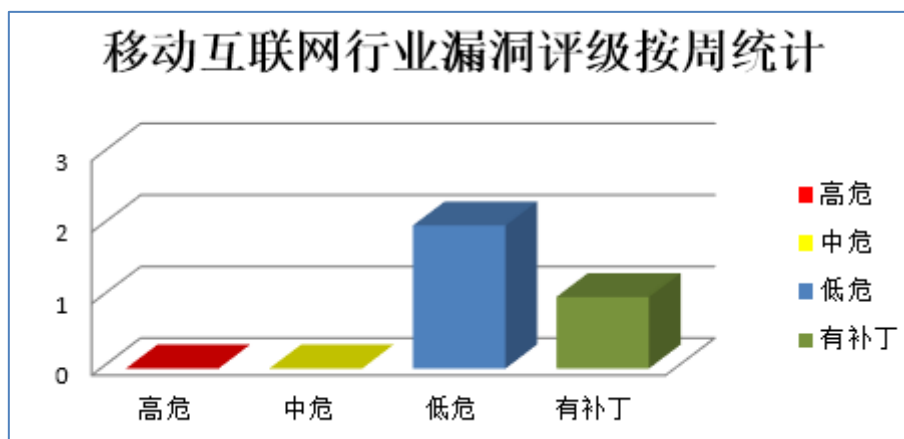


图 2 移动互联网系统行业漏洞统计

本周重要漏洞信息

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Oracle 产品安全漏洞

Oracle Sun Solaris 是美国甲骨文（Oracle）公司的一套类 Unix 操作系统。Oracle Fusion Middleware 是一套适用于云环境和传统环境的应用服务器。Oracle Database Server 是一套关系数据库管理系统。Oracle Commerce Platform 是一套电子商务解决方案平台。Oracle Java SE 用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序。本周，上述产品被披露存在拒绝服务、任意代码执行和未明漏洞。攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Oracle Sun Solaris Kernel IDMap 子组件拒绝服务漏洞、Oracle Sun Solaris Accounting commands 子组件任意代码执行漏洞、Oracle Sun Systems 产品 Sun Solaris 任意代码执行漏洞、Oracle Fusion Middleware Access Manager 组件存在未明漏洞、Oracle Database Server VM 组件存在未明漏洞、Oracle Commerce Platform Commerce Guided Search/Commerce Experience Manager 组件任意代码执行漏洞、Oracle Java SE Hotspot 任意代码执行漏洞、Oracle Java SE Deployment 子组件存在未明漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02693>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02701>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02553>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02576>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02577>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02593>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02587>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02588>

2、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司开发的一款 Web 浏览器。Google V8 是其中的一套开源 JavaScript 引擎。本周，上述产品被披露存在多个安全漏洞。攻击者可利用漏洞获取敏感信息、执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Chrome V8 拒绝服务漏洞（CNVD-2015-02649）、Google Chrome 拒绝服务漏洞（CNVD-2015-02648、CNVD-2015-02653）、Google Chrome 内存破坏漏洞（CNVD-2015-02654）、Google Chrome V8 类型混淆漏洞（CNVD-2015-02614）、Google Chrome Skia 越界写漏洞（CNVD-2015-02617）、Google Chrome 'RenderFrameImpl::OnMessageReceived' 内存错误引用漏洞、Google Chrome 信息泄露漏洞（CNVD-2015-02650）。其中，除“Google Chrome 拒绝服务漏洞（CNVD-2015-02653）、Google Chrome 信息泄露漏洞（CNVD-2015-02650）”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02649>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02648>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02653>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02654>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02614>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02617>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02618>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02650>

3、Adobe 产品安全漏洞

Adobe Flash Player 是美国奥多比（Adobe）公司的一款跨平台、基于浏览器的多媒体播放器产品。该产品支持跨屏幕和浏览器查看应用程序、内容和视频。本周，上述产品被披露存在双重释放、拒绝服务和内存错误引用漏洞。攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Adobe Flash Player 双重释放漏洞（CNVD-2015-02523、CNVD-2015-02524）、Adobe Flash Player 拒绝服务漏洞（CNVD-2015-02529、CNVD-2015-02528、CNVD-2015-02527、CNVD-2015-02526、CNVD-2015-02525）、Adobe Flash Player 内存错误引用漏洞（CNVD-2015-02519）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02523>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02524>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02529>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02528>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02527>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02526>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02525>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02519>

4、Drupal 产品安全漏洞

Drupal 是 Drupal 社区所维护的一套用 PHP 语言开发的免费、开源的内容管理系统。本周，上述产品被披露存在开放重定向、跨站脚本、跨站请求伪造漏洞。攻击者可利用漏洞重定向网站或进行跨站攻击。

CNVD 收录的相关漏洞包括：Drupal Node basket 模块开放重定向漏洞、Drupal Public Download Count 模块跨站脚本漏洞、Drupal Shibboleth Authentication 模块跨站请求伪造漏洞、Drupal Corner 模块跨站请求伪造漏洞、Drupal Amazon AWS 模块存在未明漏洞、Drupal Node Invite 模块跨站脚本漏洞、Drupal Node Invite 模块开放重定向漏洞、Drupal Node Invite 模块跨站请求伪造漏洞。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02706>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02707>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02661>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02702>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02703>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02704>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02705>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02662>

5、OrangeHRM /index.php/recruitment/viewCandidates sortField SQL 注入漏洞

OrangeHRM 是一个开源的人力资源管理工具,功能包括雇员资料管理、员工自服务系统、考勤、津贴以及招聘等功能。本周，OrangeHRM 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者利用该漏洞可提交特制的 SQL 查询,操作或获取数据库数据。目前，厂商尚未发布该漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02548>

更多高危漏洞如表 3 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。

参考链接：<http://www.cnvd.org.cn/flaw/list.htm>

CNVD 编号	漏洞名称	综合评级	修复方式
---------	------	------	------

CNVD-2015-02544	HP 存在多个权限提升漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://h20564.www2.hp.com/portal/site/hpsc/public/kb/
CNVD-2015-02545	das_watchdog 'XAUTHORITY'环境变量处理缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://github.com/kmatheussen/das_watchdog/commit/bd20bb02e75e2c http://www.openwall.com/lists/oss-security/2015/04/01/8 http://www.debian.org/security/
CNVD-2015-02542	GNU Mailman 目录遍历漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://launchpad.net/mailman/+milestone/2.1.20
CNVD-2015-02532	X.Org libX11 'MakeBigReq()'Macro 缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://cgit.freedesktop.org/xorg/lib/libX11/commit/?id=39547d600a13713e15429f49768e54c3173c828d
CNVD-2015-02599	Apport/Abrt 本地提权漏洞	高	用户可联系供应商获得补丁信息： https://fedorahosted.org/abrt/
CNVD-2015-02596	Wordpress Video Gallery SQL 注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.apptha.com/category/extension/Wordpress/Video-Gallery
CNVD-2015-02598	Wordpress Ajax Store Locator SQL 注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://codecanyon.net/item/ajax-store-locator-wordpress/5293356
CNVD-2015-02624	DBD-Firebird 栈缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.openwall.com/lists/oss-security/2015/03/30/10
CNVD-2015-02623	GNU less 'is_utf8_well_formed()'远程缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.mandriva.com/security/advisories?name=MDVSA-2015:199
CNVD-2015-02622	GLPI 目录遍历漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.glpi-project.org/spip.php?

			page=annonce&id_breve=330
--	--	--	---------------------------

表 3 部分高危漏洞列表

小结：本周，Oracle 多款产品被批露存在拒绝服务、任意代码执行和未明漏洞。攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。此外，Google、Adobe、Drupal 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、进行跨站脚本、执行任意代码、或发起拒绝服务攻击。另外，OrangeHRM 被披露存在一个高危零日漏洞，攻击者利用该漏洞可提交特制的 SQL 查询，操作或获取数据库数据。建议相关用户应随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、Microsoft 修补 Windows 产品漏洞

Microsoft Windows 7 SP1 是美国微软（Microsoft）公司发布的 Windows 7 操作系统最新的 Service Pack (SP)。SP 是一种 Windows 更新（通常与先前发行的更新合并在一起），有助于提高 Windows 的可靠性。

本周，Microsoft 修补了上述产品存在的未明漏洞，避免攻击者利用漏洞获取权限。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的网络安全事件。补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/57681>

本周要闻速递

1. 流行 iOS 网络通信库 AFNetworking 曝 SSL 漏洞

AFNetworking 是一款大名鼎鼎的开源网络库，能够让开发者们在 iOS 和 OS X 程序中加入网络功能。但是，这款库没有检查 SSL 证书是否是颁发给某个合法域名。这直接导致了任何使用了早于 2.5.3 版本的 AFNetworking 的 iOS 程序都存在漏洞，即使程序由 SSL 加密数据，黑客可以窃取和篡改数据。

参考链接：<http://www.freebuf.com/news/65744.html>

2. 安卓 WiFi 管理组件 wpa_supplicant 存在高危漏洞

流行 WLAN 无线网络管理组件 cwpa_supplicant 曝高危漏洞（CVE-2015-1863），可导致泄露内存信息、DoS 拒绝服务或任意代码执行。cwpa_supplicant 能在 Android、Linux、BSD、Mac OS X、Windows 以及部分其他操作系统上运行。该漏洞主要影响安卓系统，而其它系统也可能会受影响。

参考链接：<http://www.freebuf.com/news/65593.html>

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999