

信息安全漏洞周报

2014 年 4 月 14 日-2014 年 4 月 20 日

2014 年第 16 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 231 个，其中高危漏洞 70 个、中危漏洞 140 个、低危漏洞 21 个。上述漏洞中，可利用来实施远程攻击的漏洞有 215 个。本周收录的漏洞中，已有 218 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。本周互联网上出现 “Sendy 'send-to' SQL 注入漏洞” 等零日攻击代码，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 231 个漏洞。报送情况如表 1 所示。其中，天融信、安天实验室、启明星辰、绿盟科技等单位报送数量较多。此外，CNCERT 各分中心、习科网络安全、High-Tech Bridge Security Research 及多个白帽子向 CNVD 提交了 111 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	211	0
安天实验室	194	2
启明星辰	154	0
绿盟科技	152	0
知道创宇	69	0
恒安嘉新	48	0
习科网络安全	56	56
High-Tech Bridge Security Research	1	0

CNCERT 广东分中心	16	16
CNCERT 福建分中心	15	15
CNCERT 山西分中心	5	5
CNCERT 上海分中心	5	5
CNCERT 安徽分中心	3	3
CNCERT 贵州分中心	1	1
CNCERT 河北分中心	1	1
CNCERT 四川分中心	1	1
CNCERT 陕西分中心	1	1
个人	6	5
报送总计	939	111
录入总计	231（去重）	111

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、PaperThin、SAP 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	98	42%
2	PaperThin	16	7%
3	SAP	11	5%
4	Wordpress	8	3%
5	Juniper	7	3%
6	IBM	5	2%
7	EMC	4	2%
8	Drupal	4	2%
9	Siemens	3	1%
10	其它	75	33%

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 231 个漏洞。其中应用程序漏洞 147 个，WEB 应用漏洞 46 个，数据库漏洞 18 个，操作系统漏洞 13 个，网络设备漏洞 6 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	147

WEB 应用漏洞	46
数据库漏洞	18
操作系统漏洞	13
网络设备漏洞	6
安全产品漏洞	1

表 3 漏洞按影响类型统计表

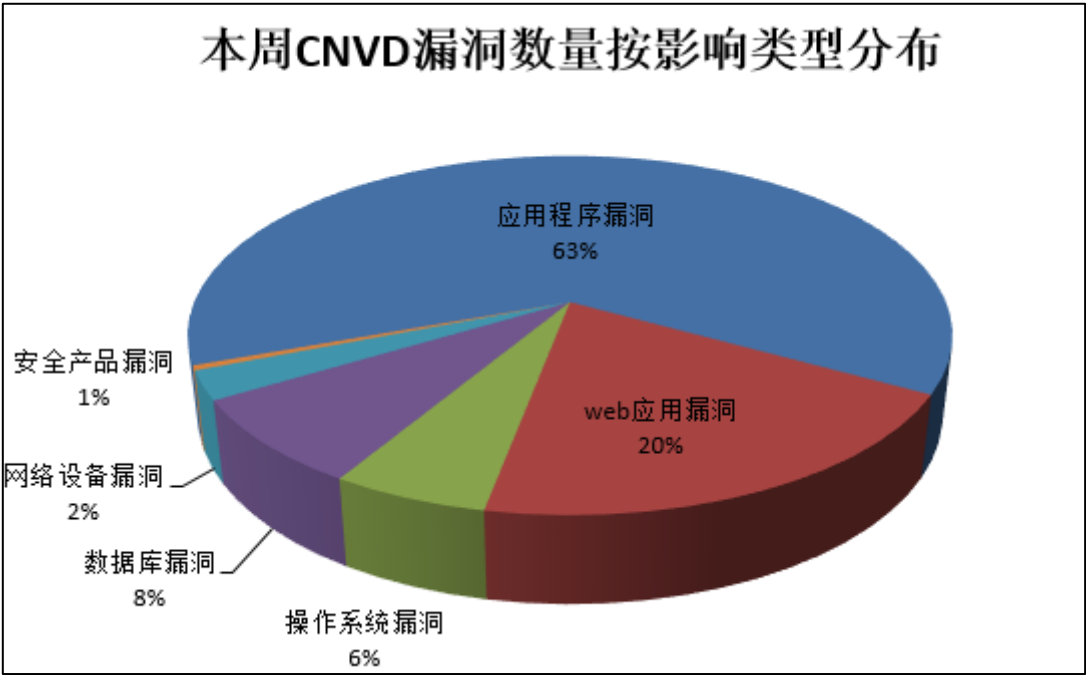


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 27 个电信行业漏洞、5 个移动互联网行业漏洞、4 个工控系统行业漏洞（如下列表所示）。其中，“Juniper JunOS IGMP 包处理拒绝服务漏、Juniper JunOS SRX 系列服务网关 flowd 拒绝服务漏洞、Oracle WebLogic Server WLS Security 子件存在未明远程漏洞、Oracle Database Server Core RDBMS 子件存在未明远程代码执行漏洞、BlackBerry 10 OS 'qconnDoor'服务堆缓冲区溢出漏洞、IOServer 越界读取漏洞、Siemens SINEMA Server 存在未明远程代码执行漏洞”的综合评级为“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-2014-02303	Juniper JunOS J-Web 存在多个跨站脚本漏洞	中	是
电信	CNVD-2014-02304	Juniper JunOS J-Web 系统监控脚本插入漏洞	中	是

电信	CNVD-2014-02307	Juniper JunOS MX 系列路由器 IP 包处理拒绝服务漏洞	中	是
电信	CNVD-2014-02308	Juniper JunOS IGMP 包处理拒绝服务漏洞	高	是
电信	CNVD-2014-02306	Juniper JunOS SRX 系列服务网关 flowd 拒绝服务漏洞	高	是
电信	CNVD-2014-02360	ZyXEL Wireless N300 Net USB Router NBG-419N 多个 UPNP 函数缓冲区溢出漏洞	高	否
电信	CNVD-2014-02387	Halon Security Router 存在多个安全漏洞	中	是
电信	CNVD-2014-02373	ZyXEL NBG-419N Router 安全绕过漏洞	中	否
电信	CNVD-2014-02389	Oracle WebLogic Server WLS Security 子件存在未明远程漏洞	高	是
电信	CNVD-2014-02413	Oracle MySQL Server Optimizer 子件存在未明远程拒绝服务漏洞 (CNVD-2014-02413)	中	是
电信	CNVD-2014-02412	Oracle MySQL Server Privileges 子件存在未明远程拒绝服务漏洞	低	是
电信	CNVD-2014-02427	Oracle MySQL Server XML 子件存在未明远程拒绝服务漏洞	中	是
电信	CNVD-2014-02426	Oracle MySQL Server Partition 子件存在未明远程拒绝服务漏洞 (CNVD-2014-02426)	中	是
电信	CNVD-2014-02425	Oracle MySQL Server Performance Schema 子件存在未明远程拒绝服务漏洞	低	是
电信	CNVD-2014-02422	Oracle MySQL Server Options 子件存在未明远程拒绝服务漏洞	低	是
电信	CNVD-2014-02421	Oracle MySQL Server Federated 子件存在未明远程拒绝服务漏洞	中	是
电信	CNVD-2014-02420	Oracle MySQL Server DML 子件存在未明远程拒绝服务漏洞	中	是
电信	CNVD-2014-02419	Oracle MySQL Server Inno	中	是

		DB 子件存在未明远程拒绝服务漏洞（CNVD-2014-02419）		
电信	CNVD-2014-02418	Oracle MySQL Server RBR 子件存在未明远程漏洞	中	是
电信	CNVD-2014-02417	Oracle MySQL Server Replication 子件存在未明远程拒绝服务漏洞（CNVD-2014-02417）	低	是
电信	CNVD-2014-02416	Oracle MySQL Server Client 子件存在未明远程漏洞	中	是
电信	CNVD-2014-02415	Oracle MySQL Server MyISAM 子件存在未明远程拒绝服务漏洞	中	是
电信	CNVD-2014-02414	Oracle MySQL Server InnoDB 子件存在未明远程漏洞	中	是
电信	CNVD-2014-02424	ZyXEL Wireless N300 Net USB Router NBG-419N management.c 远程命令注入漏洞	高	否
电信	CNVD-2014-02433	D-Link DAP-1150 index.cgi 多个参数存储型跨站脚本漏洞	中	否
电信	CNVD-2014-02454	Oracle Database Server Core RDBMS 子件存在未明远程代码执行漏洞	高	是
电信	CNVD-2014-02455	Oracle Database Server Core RDBMS 子件存在未明远程漏洞	中	是
移动互联网	CNVD-2014-02313	BlackBerry 10 OS 'qconnDoor'服务堆缓冲区溢出漏洞	高	是
移动互联网	CNVD-2014-02362	WhatsApp Messenger for iOS 非打印字符处理远程拒绝服务漏洞	中	是
移动互联网	CNVD-2014-02375	Amtelco miSecureMessages 未授权访问漏洞	高	否
移动互联网	CNVD-2014-02497	CamiApp for Android 权限访问限制绕过漏洞	中	是
移动互联网	CNVD-2014-02493	apps4u@android SD Card Manager for Android 目录遍历漏洞	中	是
工控系统	CNVD-2014-02309	IOServer 越界读取漏洞	高	是
工控系	CNVD-2014-02366	Siemens SINEMA Server 特	中	是

统		制 HTTP 请求处理远程拒绝服务漏洞		
工控系统	CNVD-2014-02365	Siemens SINEMA Server 存在未明路径遍历远程信息泄露漏洞	中	是
工控系统	CNVD-2014-02364	Siemens SINEMA Server 存在未明远程代码执行漏洞	高	是

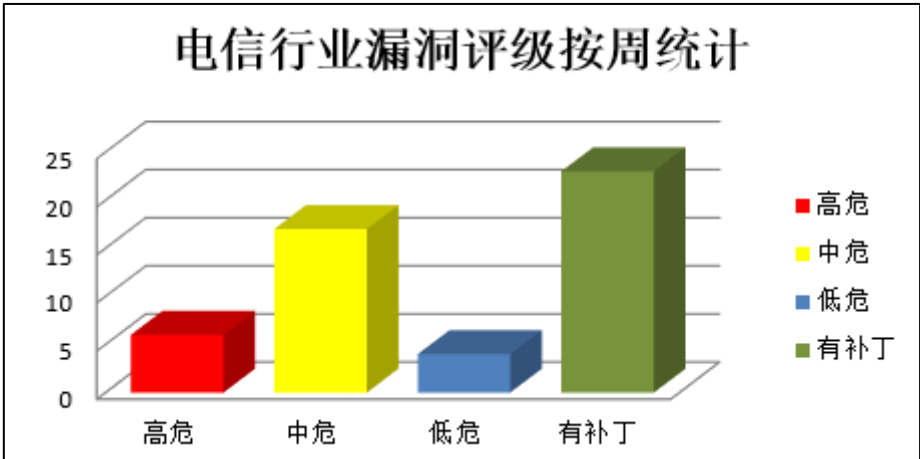


图 1 电信行业漏洞统计

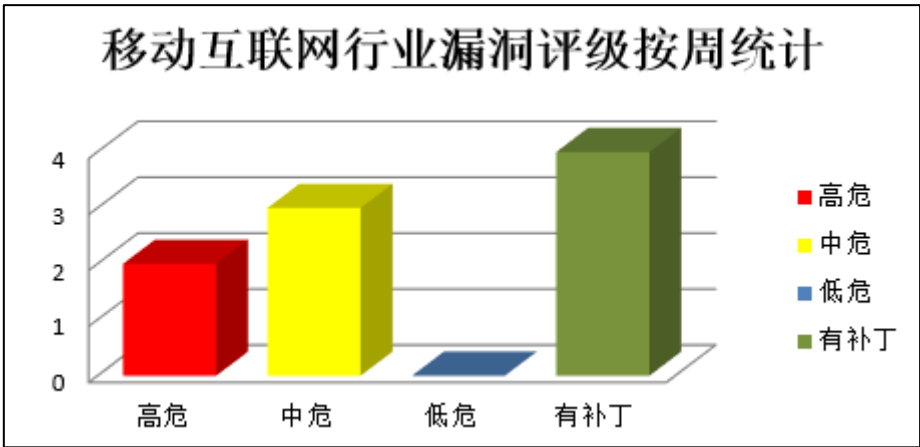


图 2 移动互联网行业漏洞统计

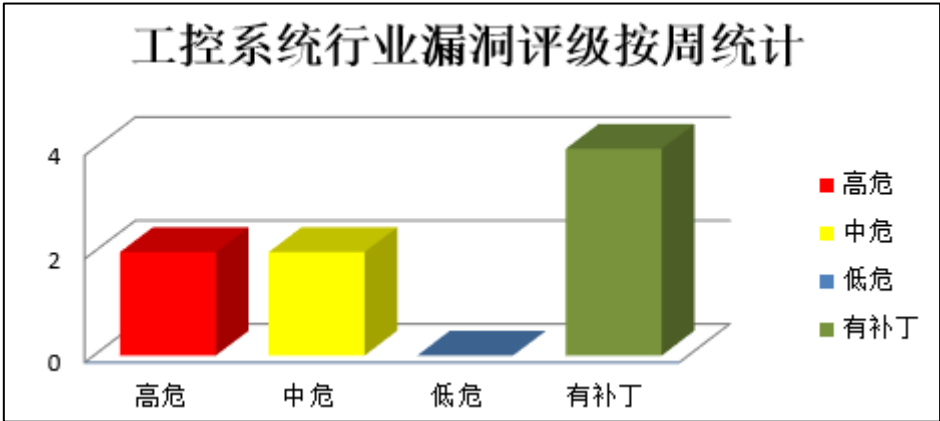


图 3 工控行业漏洞统计



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 WebLogic server 是一款应用服务器平台，用于构建和运行企业应用和服务。Oracle Java Runtime Environment 是一款为 JAVA 应用程序提供可靠的运行环境的解决方案。本周，上述产品被披露存在安全漏洞，攻击者利用漏洞发起远程攻击。

CNVD 收录的相关漏洞包括：Oracle WebLogic Server WLS Security 子件存在未明远程漏洞、Oracle Java JDK / JRE / SE Embedded Sound 子件存在未明远程漏洞、Oracle Java JDK / JRE / SE Embedded Deployment 子件存在未明远程代码执行漏洞、Oracle Java JDK / JRE / SE Embedded JAX-WS 子件存在未明漏洞、Oracle Java JDK / JRE / SE Embedded / JavaFX 2D 子件存在未明远程代码执行漏洞。上述漏洞的综合评级均为“高危”。厂商已经发布了漏洞的修补程序。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-2014-02389>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02428>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02423>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02430>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02490>

2、PaperThin 产品安全漏洞

PaperThin CommonSpot 是基于 web 的内容管理系统。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞进行未授权操作或执行任意代码。

CNVD 收录的相关漏洞包括：PaperThin CommonSpot Content Server 任意代码执行漏洞、PaperThin CommonSpot Content Server 文件上传远程代码执行漏洞、PaperThin CommonSpot Content Server URI 参数操作漏洞、PaperThin CommonSpot Content Server 存在多个安全绕过漏洞、PaperThin CommonSpot Content Server 安全绕过漏洞。上述漏洞的综合评级均为“高危”。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-2014-02510>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02517>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02516>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02518>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02519>

3、SAP 产品安全漏洞

SAP BI Universal Data Integration 是德国思爱普（SAP）公司的一套用于 SAP BI 解决方案中的通用数据分析接口。adminadapter 是该公司的一套适配器管理服务。SAP Solution Manager 是一套集系统监控、SAP 支持桌面、自助服务、ASAP 实施等多个功能为一体的系统管理平台。SAP NetWeaver 是一套面向服务的集成化应用平台。SAP Enterprise Portal 是一套基于 NetWeaver 系统平台的企业门户网站，它包含内容管理、单点登录、知识管理、协同工作、全文检索等模块。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，读写用户任意文件或修改应用程序配置，安装或删除应用程序。

CNVD 收录的相关漏洞包括：SAP Enterprise Portal 权限控制漏洞、SAP NetWeaver J2EE Engine 存在未明漏洞、SAP Solution Manager Diagnostics 代理存在未明漏洞、SAP adminadapter 存在未明漏洞、SAP BI Universal Data Integration J2EE 架构存在未明 SQL 注入漏洞。上述漏洞的综合评级均为“高危”。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-2014-02345>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02344>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02343>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02341>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02333>

4、Juniper 产品安全漏洞

Juniper Networks JUNOS 是一款 Juniper 网络公司的系列边界路由器等所运行的操作系统。Juniper JunOS SRX Branch Series Service Gateways 是系列服务网关动态服务架构产品。本周，该产品被披露存在拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Juniper JunOS SRX 系列服务网关 flowd 拒绝服务漏洞、Juniper JunOS IGMP 包处理拒绝服务漏洞、Juniper JunOS MX 系列路由器 IP 包处理拒绝服务漏洞、Juniper JunOS SRX 服务网关动态 VPN 连接拒绝服务漏洞。其中，“Juniper JunOS SRX 系列服务网关 flowd 拒绝服务漏洞、Juniper JunOS IGMP 包处理拒绝服务漏洞”的综合评级均为“高危”。厂商已发布了上述漏洞的修补程序。CNVD 提醒相关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-2014-02306>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02308>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02307>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02305>

5、Amtelco miSecureMessages 未授权访问漏洞

Amtelco miSecureMessages 是一个可用于多个移动设备上的对消息进行加密的应用。本周, Amtelco miSecureMessages 被披露存在一个综合评级为“高危”的未授权访问漏洞。由于 Amtelco miSecureMessages 对用户消息访问缺少正确的验证, 攻击者可在 XML 请求中提供 contactID 和合法许可证键值, 访问任意用户消息。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-2014-02375>

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-2014-02310	JBIG-KIT LibJbig 图像文件处理远程缓冲区溢出漏洞	高	用户可以联系供应商获得补丁信息: https://www.cl.cam.ac.uk/~mgk25/jbigkit/
CNVD-2014-02311	Sophos Web Appliance 存在多个漏洞	高	用户可以联系供应商获得补丁信息: http://www.sophos.com/
CNVD-2014-02309	IOServer 越界读取漏洞	高	用户可以联系供应商获得补丁信息: http://ioserver.com/
CNVD-2014-02313	BlackBerry 10 OS 'qconnDoor'服务堆缓冲区溢出漏洞	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: http://www.blackberry.com/
CNVD-2014-02315	vSphere 客户端任意文件下载漏洞	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: http://www.vmware.com/
CNVD-2014-02328	Dillo 图像处理整数溢出漏洞	高	Dillo 3.0.4 已修复此漏洞, 建议用户下载使用: http://www.dillo.org/
CNVD-2014-02331	CyaSSL 存在多个未明漏洞	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: http://www.wolfssl.com/yaSSL/Home.html
CNVD-2014-02334	SolarWinds Network Performance Monitor 'wpdlx'远程代码执行漏洞	高	SolarWinds Network Performance Monitor 10.7 已修复此漏洞, 建议用户下载使用: http://www.solarwinds.com/documentation/Orion/docs/ReleaseNotes/relea

			seNotes.htm
CNVD-2014-02347	Tigase 拒绝服务漏洞	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.tigase.org/content/uncontrolled-resource-consumption-highly-compressed-xmpp-messages
CNVD-2014-02348	Erlang Solutions MongooseIM 拒绝服务漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://www.erlang-solutions.com/products/mongooseim-massively-scalable-ejabberd-platform

表 3 部分高危漏洞列表

小结：本周，Oracle 被披露存在多个安全漏洞，攻击者可利用漏洞发起远程攻击。此外，PaperThin、SAP、Juniper 集中披露多款产品存在多个漏洞，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。另外，Amtelco miSecureMessages 被披露存在一个高危零日漏洞，攻击者可利用漏洞在 XML 请求中提供 contactID 和合法许可证键值，访问任意用户消息。CNVD 已经建议相关用户应随时关注厂商主页，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、Apache 修补 Syncope 产品漏洞

Apache Syncope 是用于企业环境的数字身份管理，在 JEE 技术的实施和 Apache 2.0 许可下发布的开源系统。

本周，Apache 修补了上述产品存在的远程代码执行漏洞，避免远程攻击者通过运行 Apache Syncope core 的 JEE container 来执行任意代码。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/44913>

本周要闻速递

1. 三星 Galaxy S5 指纹传感器被黑

4 月 16 日消息，据国外媒体报道，来自 Security Research Labs 的专家们周二在 YouTube 上放出一段视频，展示了其如何利用去年早些时候在苹果 iPhone 5s 上使用过的

方法，成功绕过三星 S5 的指纹认证系统。该安全机构通过可拍照手机和橡胶膜制作了一个“假指纹”，这成功骗过了 Galaxy S5 指纹传感器，并获得该手机的主页面访问权及 PayPal 应用访问权。其中，PayPal 应用通过指纹认证可向他人转账。

参考链接：<http://stock.jrj.com.cn/2014/04/16082617051604.shtml>

2. 谷歌向 OEM 推动 Android 安全补丁

4 月 17 日消息：日前，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。

参考链接：<http://soft.zol.com.cn/447/4476587.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