

信息安全漏洞周报

2014 年 7 月 28 日-2014 年 8 月 3 日

2014年第31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**低**。

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 121 个，其中高危漏洞 29 个、中危漏洞 84 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 108 个。本周收录的漏洞中，已有 78 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“WordPress 插件 Slider Revolution Responsive 'img' 参数任意文件下载漏洞”、“Fonality trixbox 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 5 家成员单位、合作伙伴及个人报送了本周收录的全部 121 个漏洞。报送情况如表 1 所示。其中，奇虎 360、天融信、恒安嘉新、启明星辰、安天实验室等单位报送数量较多。此外，CNCERT 各分中心、High-Tech BridgeSecurity Research 及白帽子向 CNVD 提交了 245 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	235	235
天融信	126	0
恒安嘉新	95	0
启明星辰	92	0
安天实验室	78	0
绿盟科技	55	0

High-Tech Bridge Security Research	1	1
CNCERT 山西分中心	4	4
CNCERT 福建分中心	2	2
CNCERT 山东分中心	1	1
个人	2	2
报送总计	691	245
录入总计	121（去重）	245

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 IBM、Cisco、WordPress 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	IBM	10	8%
2	Cisco	10	8%
3	WordPress	8	7%
4	SAP	6	5%
5	Siemens	5	4%
6	Linux	3	2%
7	Drupal	3	2%
8	Linux	3	2%
9	Apache	2	2%
10	其他	71	60%

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 121 个漏洞。其中应用程序漏洞 66 个，WEB 应用漏洞 30 个，网络设备漏洞 13 个，安全产品漏洞 7 个，操作系统漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	66
WEB 应用漏洞	30
网络设备漏洞	13
安全产品漏洞	7
操作系统漏洞	5

表 3 漏洞按影响类型统计表

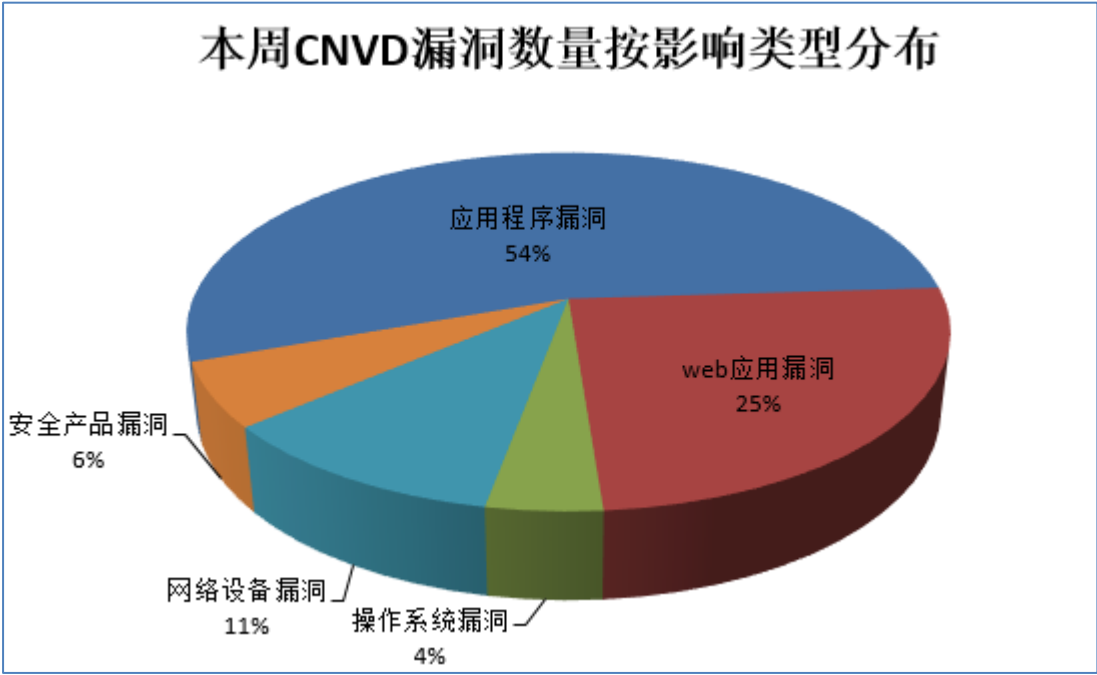


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 12 个电信行业漏洞，5 个移动互联网漏洞，10 个工控系统漏洞（如下图表所示）。其中，“IBM WebSphere Portal SQL 注入漏洞、Siemens 多款产品本地权限提升漏洞”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-2014-04647	NETGEAR DGN2200 密码信息泄露漏洞	中	否
电信	CNVD-2014-04664	IBM WebSphere Portal 远程信息泄露漏洞	中	是
电信	CNVD-2014-04673	Cisco WebEx Meetings Server 信息泄露漏洞（CNVD-2014-04673）	中	否
电信	CNVD-2014-04674	Cisco WebEx Meetings Server 信息泄露漏洞（CNVD-2014-04674）	中	否
电信	CNVD-2014-04678	Sagem F@st 3304-V1 拒绝服务漏洞	中	否
电信	CNVD-2014-04692	Cisco WebEx Meetings Server 'user.php'信息泄露漏洞	中	否
电信	CNVD-2014-04691	Cisco WebEx Meetings Server 跨站请求伪造漏洞	中	否
电信	CNVD-2014-04687	Cisco Unified Presence Server 远程拒绝服务漏洞	中	否

电信	CNVD-2014-04703	IBM WebSphere Portal 开放重定向漏洞	中	是
电信	CNVD-2014-04718	IBM WebSphere Portal 跨站脚本漏洞	中	是
电信	CNVD-2014-04717	IBM WebSphere Portal SQL 注入漏洞	高	是
电信	CNVD-2014-04753	Cisco Prime Data Center Network Manager (DCNM)跨站脚本漏洞	中	是
移动互联网	CNVD-2014-04675	Google Android 'SQLiteDatabase.java'远程安全绕过漏洞	中	否
移动互联网	CNVD-2014-04719	Seeds acmailer 跨站请求伪造漏洞	中	是
移动互联网	CNVD-2014-04734	Apple iOS 'Content-Disposition'报头跨站脚本漏洞	中	否
移动互联网	CNVD-2014-04741	Instagram for Android 会话劫持漏洞	中	否
移动互联网	CNVD-2014-04761	SavySoda WiFi HD 存在多个漏洞	中	否
工控系统	CNVD-2014-04644	Siemens SIMATIC 多个产品远程权限提升漏洞	中	是
工控系统	CNVD-2014-04643	Siemens SIMATIC WinCC 和 PCS7 权限提升漏洞	中	是
工控系统	CNVD-2014-04662	Siemens SIMATIC WinCC 和 PCS7 WebNavigator Server 信息泄露漏洞	中	是
工控系统	CNVD-2014-04663	Siemens 多款产品数据库服务器远程权限提升漏洞	中	是
工控系统	CNVD-2014-04695	Siemens 多款产品本地权限提升漏洞	高	是
工控系统	CNVD-2014-04708	Schneider Modicon M340 Web 服务器用户名/口令明可修改漏洞	高	否
工控系统	CNVD-2014-04709	Schneider Modicon M340 FTP 服务器固定用户口令漏洞	中	否
工控系统	CNVD-2014-04710	Schneider Modicon M340 Web 服务器隐藏信息泄露漏洞	中	否
工控系统	CNVD-2014-04730	Omron NS series HMI Terminals HTML 注入漏洞	低	是
工控系统	CNVD-2014-04727	Omron NS series HMI Terminals 跨站请求伪造漏洞	中	是

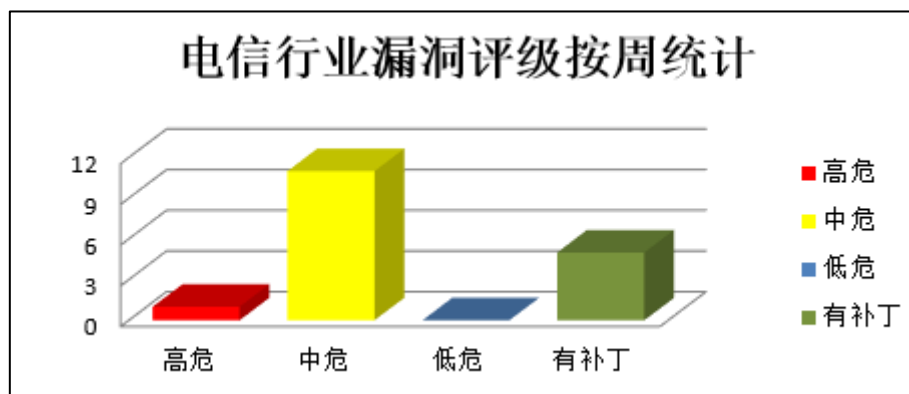


图 1 电信行业漏洞统计

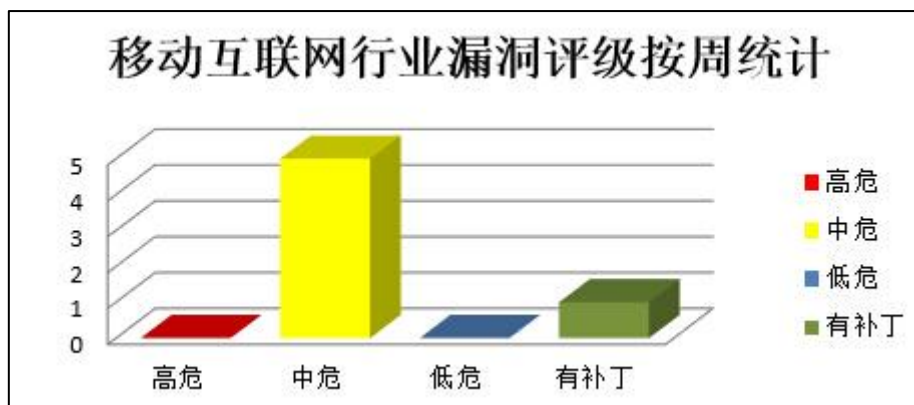


图2 移动互联网行业漏洞统计

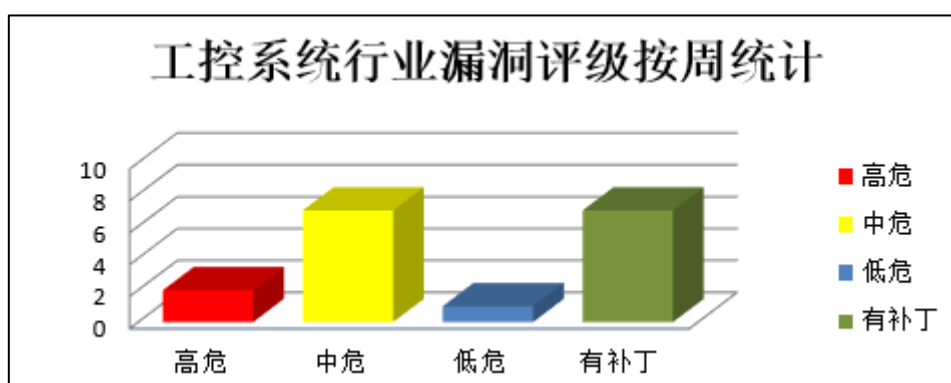


图3 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM Information Lifecycle Governance (ILG) 是美国 IBM 公司的一套信息生命周期治理解决方案。IBM Maximo Asset Management 是美国 IBM 公司的一套综合性资产生命周期和维护管理解决方案。IBM WebSphere Portal 提供了一个组合应用程序或业务 mashup 框架，并且提供了一种高级工具来构造灵活的，基于 SOA 的解决方案。IBM Sametime 是美国 IBM 公司的一套下一代社交通信工具。该工具通过集成音频语音、数据和视频，帮助用户实现实时业务协作。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，进行跨站脚本攻击或执行任意脚本代码。

CNVD 收录的相关漏洞包括：IBM WebSphere Portal SQL 注入漏洞、IBM Atlas Suite 跨站脚本漏洞、IBM Maximo Asset Management CRLF 注入漏洞、IBM WebSphere Portal 跨站脚本漏洞、IBM Sametime Classic Meeting Server 信息泄露漏洞、IBM Sametime Classic Meeting Server 跨站脚本漏洞、IBM WebSphere Portal 远程信息泄露漏

洞、IBM WebSphere Portal 开放重定向漏洞。其中“IBM WebSphere Portal SQL 注入漏”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-2014-04717>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04738>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04737>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04718>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04666>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04665>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04664>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04703>

2、Cisco 产品安全漏洞

Cisco Prime 网络管理系统是业界最全面的管理平台，可提供融合的用户、访问和身份管理功能，同时有助于全面了解端点的连接情况。Cisco WebEx Meetings Server 是一款思科公司推出的思科会议中心实现。Cisco IOS XR 是 Cisco IOS 软件家族的一员，使用基于微内核分配操作系统架构。Cisco TelePresence 是思科公司开发的网真会议解决方案。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、发起拒绝服务攻击或执行任意脚本代码。

CNVD 收录的相关漏洞包括：Cisco IOS XR Software NetFlow 处理拒绝服务漏洞、Cisco Prime Data Center Network Manager (DCNM) 跨站脚本漏洞、Cisco WebEx Meetings Server 信息泄露漏洞、Cisco TelePresence Server 跨站脚本漏洞、Cisco WebEx Meetings Server 信息泄露漏洞（CNVD-2014-04674、CNVD-2014-04673）、Cisco WebEx Meetings Server 跨站请求伪造漏洞、Cisco WebEx Meetings Server 'user.php' 信息泄露漏洞。其中“Cisco IOS XR Software NetFlow 处理拒绝服务漏洞”的综合评级为“高危”。目前，“Cisco IOS XR Software NetFlow 处理拒绝服务漏洞、Cisco Prime Data Center Network Manager (DCNM) 跨站脚本漏洞、Cisco WebEx Meetings Server 信息泄露漏洞、Cisco TelePresence Server 跨站脚本漏洞”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-2014-04684>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04753>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04733>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04658>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04674>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04673>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04691>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04692>

3、SAP 产品安全漏洞

SAP NetWeaver 是一款 SAP 业务套件解决方案、SAP xApps 组合应用、合作伙伴解决方案以及客户定制应用的技术基础。SAP FI 模块是 SAP 中外部会计模块。SAP HANA Extended Application Services 是 SAP 公司的一款扩展应用服务器。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。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、进行未经授权操作或执行任意代码。

CNVD 收录的相关漏洞包括：SAP NetWeaver Business Warehouse 未经授权访问漏洞、SAP FI Manager Self-Service 内置编码安全绕过漏洞、SAP HANA Extended Application Services 存在多个跨站脚本漏洞、SAP HANA Extended Application Services 信息泄露漏洞（CNVD-2014-04748、CNVD-2014-04745）、SAP Solution Manager SAP_JTECH S 访问绕过漏洞。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-2014-04760>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04759>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04749>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04748>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04745>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04747>

4、Siemens 产品安全漏洞

Siemens SIMATIC WinCC 是一款能为工业领域提供完备的监控与数据采集（SCADA）功能，涵盖单用户系统直到支持冗余服务器和远程 Web 客户机解决方案的多用户系统。本周，上述产品被披露存在信息泄漏和权限提升漏洞，攻击者可利用漏洞获得敏感信息或提升权限。

CNVD 收录的相关漏洞包括：Siemens 多款产品本地权限提升漏洞、Siemens SIMATIC WinCC 和 PCS7 WebNavigator Server 信息泄露漏洞、Siemens SIMATIC WinCC 和 PCS7 权限提升漏洞、Siemens 多款产品数据库服务器远程权限提升漏洞、Siemens SIMATIC 多个产品远程权限提升漏洞。其中“Siemens 多款产品本地权限提升漏洞”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-2014-04695>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04662>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04643>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04663>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04644>

5、Parallels Tools 本地权限提升漏洞

Parallels Desktop 是一款 Mac 电脑上最强的虚拟机软件。本周，Parallels Desktop 被披露存在综合评级为“高危”的本地权限提升漏洞。攻击者利用漏洞在受影响的应用程序上下文中执行任意代码，以提升权限。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-2014-04743>

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-2014-04654	WordPress WP Backup Plus 插件任意文件下载漏洞	高	暂无
CNVD-2014-04648	Omeka '/admin/items/add'任意文件上传漏洞	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://en.wikipedia.org/wiki/Omeka
CNVD-2014-04657	WordPress 插件 Video Gallery 存在多个漏洞	高	暂无
CNVD-2014-04659	Sabre AirCentre Crew 'CWPLogin.aspx'存在多个 SQL 注入漏洞	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.sabreairlinesolutions.com/home/software_solutions/product/crew_management/
CNVD-2014-04667	Fonality trixbox SQL 注入漏洞	高	暂无
CNVD-2014-04672	Pligg CMS 'recover.php' SQL 注入漏洞	高	暂无
CNVD-2014-04676	Oxwall 远程代码执行漏洞	高	暂无
CNVD-2014-04740	多个 HP 及 H3C VPN 防火墙模块产品拒绝服务漏洞	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://itrc.hp.com https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c03993467 https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId

			=emr_na-c03993467
CNVD-2014-04689	Bugzilla 跨站请求伪造漏洞	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.bugzilla.org/
CNVD-2014-04715	WordPress 插件 Lead Octopus Power 'id' 参数 SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，IBM 多款产品披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息，进行跨站脚本攻击或执行任意脚本代码。此外，Cisco、SAP、Siemens 多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码，获取敏感信息或发起拒绝服务攻击。另外，Parallels Desktop 被披露存在一个高危零日漏洞。攻击者可以利用漏洞在受影响的应用程序上下文中执行任意代码，以提升权限。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、HP 修补 Network Virtualization、Data Protector 产品漏洞

HP Network Virtualization（也称 Shunra Network Virtualization）是美国惠普（HP）公司的一套用于发现、模拟和测试影响最终用户和应用服务的真实网络状况的应用性能测试解决方案。HP Data Protector 软件是一款成熟的企业级数据保护平台，可不受距离限制通过磁盘或磁带自动执行高性能备份和恢复。

本周，HP 修补了上述产品存在的目录遍历漏洞，避免远程攻击者利用漏洞通过特制的输入读取或删除任意文件。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/48017>
<http://www.cnvd.org.cn/patchInfo/show/48016>
<http://www.cnvd.org.cn/patchInfo/show/47969>

本周要闻速递

1. 苹果、安卓连爆安全漏洞

日前，有消息指出，继苹果(96.13, 0.53, 0.55%)的 IOS 系统被爆存在“后门”之后，谷歌(566.07, -5.53, -0.97%)的安卓操作系统又被爆出存在一项安全漏洞，可以让黑客假

冒受信任的正规应用，从而劫持用户的智能手机或平板电脑。第三方安全公司也在报告中表示，漏洞的根本问题在于安卓系统校验应用身份时采取的方式。安全公司称，每一款安卓应用都有自己的数字签名，也就是 ID 卡，当一款应用亮出 ID 时，安卓不会去向所有人核实该 ID 的真实性。也就是说，网络犯罪分子可以利用假冒的签名来开发恶意软件，从而感染用户的系统。黑客甚至还可以创建一个假冒谷歌钱包的恶意应用，然后访问用户的支付账号和财务数据。

参考链接：<http://tech.sina.com.cn/t/2014-07-31/07199527485.shtml>

2. 赛门铁克专业安全软件被曝多处漏洞

据报道，赛门铁克的安全软件《Symantec Endpoint Protection》存在安全漏洞。目前并没有全部公布，一部分被上报给了美国国土安全部旗下的电脑警备小组 US-CERT，另一部会等到本月在拉斯维加斯举行的黑帽技术大会上公布。同时在 Offensive Security 公布的信息中显示，Endpoint Protection 的一项漏洞涉及权限管理，黑客可借此获取系统的最高管理权限。赛门铁克方面表示，该漏洞威胁程度中等，目前已开始紧急修补，好在没有发现由此产生的攻击事件。

参考链接：<http://news.mydrivers.com/1/314/314833.htm>

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