

信息安全漏洞周报

2015 年 08 月 03 日-2015 年 08 月 09 日

2015 年第 32 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 86 个，其中高危漏洞 46 个、中危漏洞 36 个、低危漏洞 4 个。上述漏洞中，可利用来实施远程攻击的漏洞有 77 个。本周收录的漏洞中，已有 60 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“Foxit Reader 任意代码执行漏洞”、“php File Manager 存在多个漏洞”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 86 个漏洞。报送情况如表 1 所示。其中，奇虎、启明星辰、安天实验室、天融信、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、中国科学院院信息工程研究所第六研究室、深圳市深信服电子科技有限公司、北京国舜科技股份有限公司、乌云、漏洞盒子及白帽子向 CNVD 提交了 600 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎	298	298
启明星辰	73	0
安天实验室	51	0
天融信	49	0
恒安嘉新	45	0

绿盟科技	38	0
乌云	241	241
漏洞盒子	26	26
中国科学院信息工程研究所第六研究室	3	3
深圳市深信服电子科技有限公司	2	2
北京国舜科技股份有限公司	1	1
CNCERT 甘肃分中心	4	4
CNCERT 福建分中心	4	4
CNCERT 上海分中心	4	4
CNCERT 江西分中心	1	1
个人	16	16
报送总计	856	600
录入总计	86（去重）	600

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 General Electric Company、IBM、Symantec 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	General Electric Company	13	15%
2	IBM	13	15%
3	Cisco	9	10%
4	Symantec	7	8%
5	SO Planning	5	6%
6	WordPress	5	6%
7	Linux	3	4%
8	Webservice-DIC	3	4%
9	FreeBSD	2	2%

10	其他	26	30%
----	----	----	-----

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 86 个漏洞。其中应用程序漏洞 49 个,网络设备漏洞 15 个, WEB 应用漏洞 8 个, 安全产品漏洞 8 个, 操作系统漏洞 6 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	49
网络设备漏洞	15
WEB 应用漏洞	8
安全产品漏洞	8
操作系统漏洞	6

表 3 漏洞按影响类型统计表

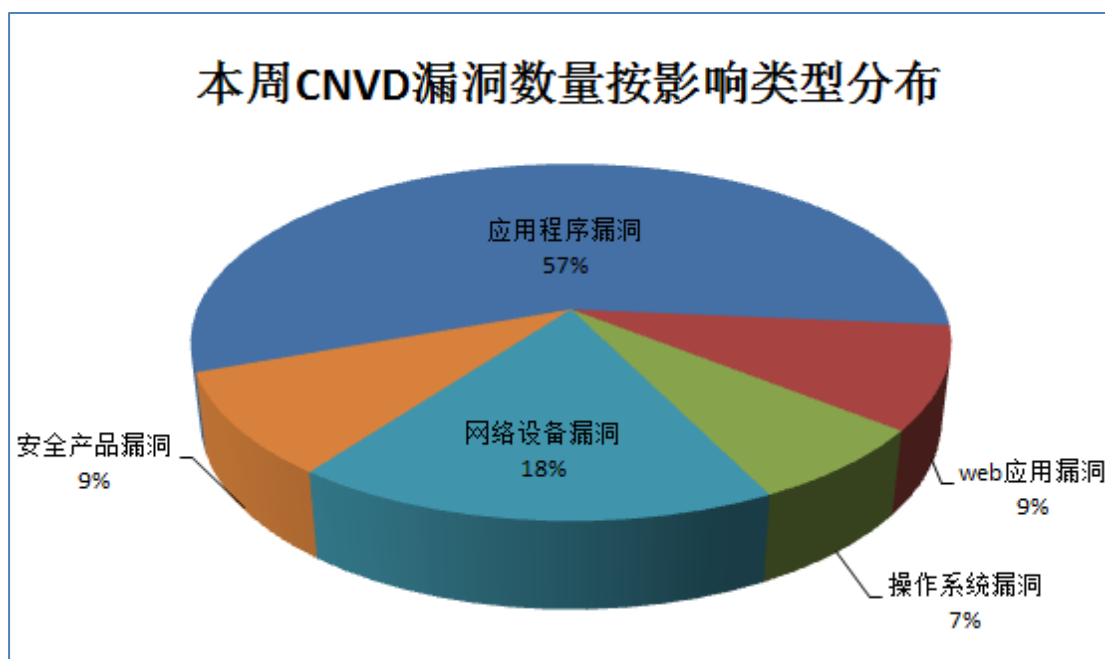


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周, CNVD 收录了 13 个电信行业漏洞, 1 个移动互联网行业漏洞, 1 个工控系统行业漏洞 (如下图表所示)。其中, “多个 D-Link 产品 HTTP 缓冲区溢出漏洞、多个 D-Link 产品 UPnP 缓冲区溢出漏洞、IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-05100、CNVD-2015-05099、CNVD-2015-05098、CNVD-2015-05097、CNVD-2015-05101)、Cisco ASR 1000 Series Aggregation Services Routers 拒绝服务漏洞”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-2015-05076	多个 D-Link 产品 HTTP 缓冲区溢出漏洞	高	是
电信	CNVD-2015-05077	多个 D-Link 产品 UPnP 缓冲区溢出漏洞	高	是
电信	CNVD-2015-05100	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-05100)	高	是
电信	CNVD-2015-05099	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-05099)	高	是
电信	CNVD-2015-05098	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-05098)	高	是
电信	CNVD-2015-05097	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-05097)	高	是
电信	CNVD-2015-05101	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞 (CNVD-2015-05101)	高	是
电信	CNVD-2015-05096	Cisco IOS XE 拒绝服务漏洞	中	是
电信	CNVD-2015-05095	Cisco ASR 1000 Series Aggregation Services Routers 拒绝服务漏洞	高	是
电信	CNVD-2015-05104	Cisco AnyConnect Secure Mobility Client 目录遍历漏洞	中	是
电信	CNVD-2015-05103	Cisco Unified Communications Manager 信息泄露漏洞 (CNVD-2015-05103)	中	否
电信	CNVD-2015-05118	IBM WebSphere eXtreme Scale 拒绝服务漏洞	中	是
电信	CNVD-2015-05119	IBM WebSphere DataPower XC10 存在未明漏洞	低	是
移动互联网	CNVD-2015-05117	Android mediaserver 服务整数溢出拒绝服务漏洞	中	是
工控系统	CNVD-2015-05102	Schneider Electric InduSoft 密码存储漏洞	中	是

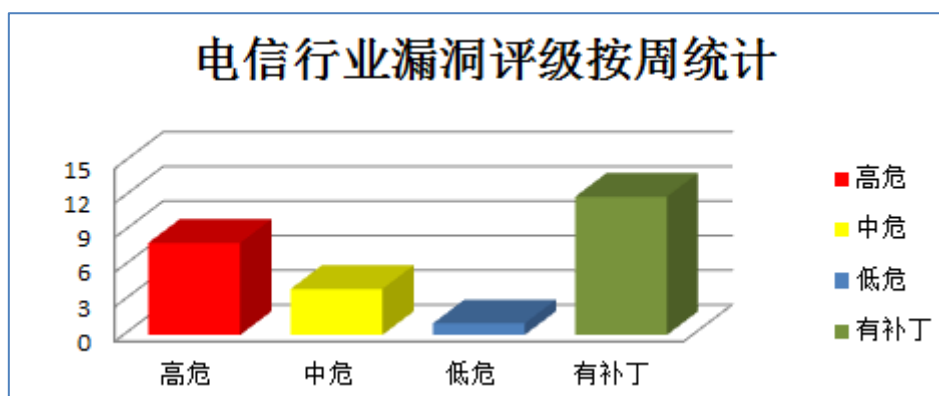


图 1 电信行业漏洞统计

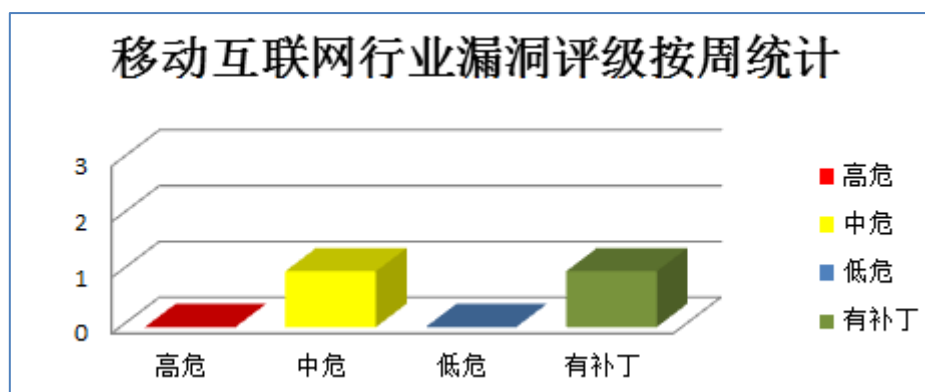


图 2 移动互联网行业漏洞统计

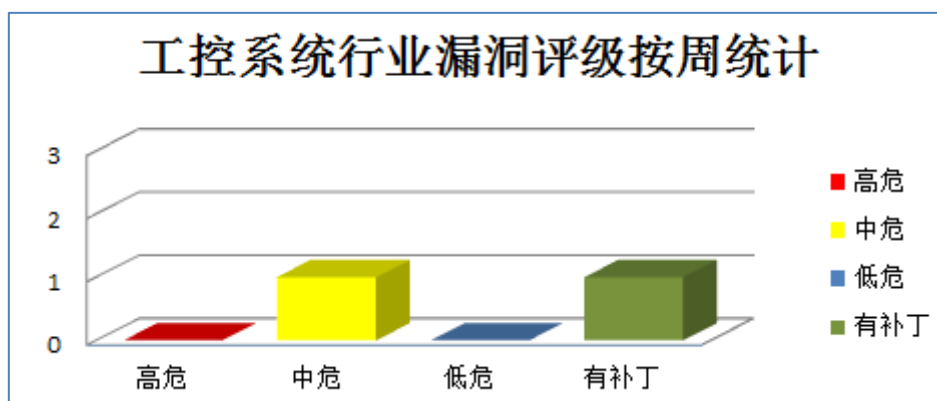


图 3 工控系统行业漏洞统计

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 MQ Light 是美国 IBM 公司的一个基于 IBM Bluemix（在云上创建、部署和管理应用程序的 PaaS 平台）的消息服务。IBM WebSphere DataPower XC10 是美国 IBM 公司的一套高速缓存平台。该平台可在对现有应用程序几乎不做任何更改的情况下对数据进行分布式高速缓存。IBM WebSphere eXtreme Scale 是美国 IBM 公司的一套分布式高速缓存解决方案。该方案提供高性能、可扩展的高速缓存框架和网格技术，可处理海量事务、降低数据库的性能限制等。IBM Business Process Manager (BPM) 是美国 IBM 公司的一套综合的业务流程管理平台。该平台为业务的流程建模、组装、监控和部署提供了一系列的相关工具。IBM SDK 是一套用于创建、发现、调用和测试 Web 服务的集成工具包。本周，上述产品被披露存在信息泄露、安全绕过和拒绝服务漏洞。攻击者利用漏洞可获得敏感信息、绕过安全限制和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM MQ Light 拒绝服务漏洞（CNVD-2015-05123、CNVD-2015-05122、CNVD-2015-05120、CNVD-2015-05121）、IBM WebSphere DataPo

wer XC10 存在未明漏洞、IBM WebSphere eXtreme Scale 拒绝服务漏洞、IBM Business Process Manager 安全绕过漏洞、IBM SDK Java Security Components 本地信息泄露漏洞。其中，“IBM MQ Light 拒绝服务漏洞（CNVD-2015-05123、CNVD-2015-05122、CNVD-2015-05120）”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-2015-05123>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05122>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05120>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05121>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05119>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05118>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05112>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05090>

2、Symantec 产品安全漏洞

Symantec Endpoint Protection Manager（SEPM）是美国赛门铁克（Symantec）公司的一套企业级病毒防护软件。该软件可防范恶意攻击，如病毒、蠕虫、特洛伊木马等。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞可获得敏感信息、提升权限或绕过身份验证。

CNVD 收录的相关漏洞包括：Symantec Endpoint Protection Manager 不可信搜索路径漏洞、Symantec Endpoint Protection Manager SQL 注入漏洞、Symantec Endpoint Protection Manager 目录遍历漏洞、Symantec Endpoint Protection Manager 权限获取漏洞、Symantec Endpoint Protection Manager 任意文件读取漏洞、Symantec Endpoint Protection Manager 任意文件写入漏洞、Symantec Endpoint Protection Manager 验证绕过漏洞。其中，除“Symantec Endpoint Protection Manager 不可信搜索路径漏洞、Symantec Endpoint Protection Manager 验证绕过漏洞”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-2015-05111>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05110>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05109>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05108>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05107>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05106>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05105>

3、Cisco 产品安全漏洞

Cisco IM and Presence Service 是美国思科（Cisco）公司的一套可提供企业级即时通讯和网络显现服务的软件。Cisco Prime Central for Hosted Collaboration Solution(PC4HCS) 是美国思科（Cisco）公司的一套电信级的、可扩展的服务保证管理平台。该平台提供安全接入认证、实时故障分析等功能。Cisco Unified Communications Manager 是企业级 IP 电话呼叫处理系统。Cisco AnyConnect Secure Mobility Client 是思科下一代 VPN 客户端。Cisco ASR1000 系列汇聚服务路由器，提供了广域网边缘解决方案，将信息、通信、协作和商务融为一体。Cisco IOS XE 是美国思科（Cisco）公司为其网络设备开发的操作系统。Cisco Firepower Extensible Operating System on Firepower 9000 device 是美国思科（Cisco）公司的一套运行于 9000 系列防火墙设备中的操作系统。Cisco Web Security Appliance（WSA）、Email Security Appliance（ESA）和 Content Security Management Appliance（SMA）都是美国思科（Cisco）公司的产品。Cisco WSA 是一套 Web 安全设备。ESA 是一套电子邮件安全设备。Content SMA 是一套内容安全管理设备。本周，上述产品被披露存在信息泄露、目录遍历、跨站脚本和拒绝服务漏洞。攻击者可利用漏洞获得敏感信息、进行跨站脚本攻击和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IM and Presence Service 跨站脚本漏洞、Cisco Prime Central for Hosted Collaboration Solution 跨站脚本漏洞、Cisco Unified Communications Manager 信息泄露漏洞（CNVD-2015-05103）、Cisco AnyConnect Secure Mobility Client 目录遍历漏洞、Cisco ASR 1000 Series Aggregation Services Routers 拒绝服务漏洞、Cisco IOS XE 拒绝服务漏洞、Cisco Firepower 9000 Series 设备信息泄露漏洞、多个 Cisco 产品跨站脚本漏洞（CNVD-2015-05073）。其中，“Cisco ASR 1000 Series Aggregation Services Routers 拒绝服务漏洞”的综合评级为“高危”。目前，除“Cisco Unified Communications Manager 信息泄露漏洞（CNVD-2015-05103）、Cisco Firepower 9000 Series 设备信息泄露漏洞”外，厂商已经发布了其余漏洞的修补程序。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-2015-05114>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05113>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05103>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05104>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05095>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05096>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05066>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05073>

4、GE 产品安全漏洞

GE Healthcare Centricity Image Vault 是美国通用电气（GE）公司的一个用于医疗行业的 Vivid 心血管超声图片库。GE Healthcare Centricity DMS 是美国通用电气（GE）公

司的一套用于医疗行业的心脏病临床教育数据管理系统。GE Healthcare Centricity PACS 是美国通用电气（GE）公司的一套用于医疗行业的影像归档及传输系统（PACS）。Workstation 是一个 PACS 工作站；Server 是一个 PACS 服务器。GE Healthcare Centricity PACS Workstation 是美国通用电气（GE）公司的一款用于医疗行业的影像归档及传输系统（PACS）工作站。GE Healthcare Centricity Clinical Archive Audit Trail Repository 是美国通用电气（GE）公司的一个用于医疗行业的临床归档审计跟踪库。GE Healthcare eNTEGRA P&R（Processing & Review）是美国通用电气（GE）公司的一套用于医疗行业的医用核计算机系统。本周，上述产品被披露存在信任管理漏洞。攻击者可利用漏洞控制设备。

CNVD 收录的相关漏洞包括：GE Healthcare Centricity Image Vault 信任管理漏洞、GE Healthcare Centricity DMS 信任管理漏洞、GE Healthcare Centricity PACS Workstation 和 Server 信任管理漏洞、GE Healthcare Centricity PACS Workstation 信任管理漏洞（CNVD-2015-05140）、GE Healthcare Centricity DMS Ad Hoc Reporting 信任管理漏洞、GE Healthcare Centricity PACS Workstation 信任管理漏洞、GE Healthcare Centricity Clinical Archive Audit Trail Repository 信任管理漏洞、GE Healthcare eNTEGRA P&R 信任管理漏洞。上述漏洞的综合评级为“高危”。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-2015-05144>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05142>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05141>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05140>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05138>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05137>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05134>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05149>

5、Apple OS X 权限提升 0day 漏洞

Apple OS X（前称 Mac OS X）是苹果公司为麦金塔电脑开发的专属操作系统的最新版本。本周，Apple OS X 被披露存在综合评级为“高危”的权限提升漏洞。攻击者利用该漏洞可用 root 权限执行 shell 命令，安装恶意软件及广告软件。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-2015-05148>

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-2015-05071	Snorby 'view.html.erb' HTML 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： https://github.com/Snorby/snorby
CNVD-2015-05079	SO Planning 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.soplanning.org/en/download.php
CNVD-2015-05086	Webservice-DIC yoyaku_v41 输入验证漏洞	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.d-ic.com/
CNVD-2015-05085	Webservice-DIC yoyaku_v41 操作系统命令注入漏洞	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.d-ic.com/
CNVD-2015-05083	SO Planning PHP 代码注入漏洞	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.soplanning.org/en/download.php
CNVD-2015-05093	FreeBSD TCP 重组内存消耗漏洞	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： https://security.FreeBSD.org/advisories/FreeBSD-SA-15:15.tcp.asc
CNVD-2015-05094	FreeBSD patch 远程命令执行漏洞	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： https://security.FreeBSD.org/advisories/FreeBSD-SA-15:14.bsdpatch.asc
CNVD-2015-05125	多款 Chiyu 产品跨站脚本漏洞	高	暂无
CNVD-2015-05126	多款 Chiyu 产品 fingerprint access-control 设备存在漏洞	高	暂无
CNVD-2015-05133	多款 GE 产品信任管理漏洞（CNVD-2015-05133）	高	暂无

表 3 部分高危漏洞列表

小结：本周，IBM 产品被披露存在信息泄露、安全绕过和拒绝服务漏洞。攻击者利用漏洞可获得敏感信息、绕过安全限制和发起拒绝服务攻击。此外，Symantec、Cisco、GE 多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息、提升权限、进行跨站脚本攻击或发起拒绝服务攻击。另外，Apple OS X 被披露存在一个高危零日漏洞，攻击者利用该漏洞可用 root 权限执行 shell 命令，安装恶意软件及广告软件。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、OpenSSH 修补 OpenSSH 产品漏洞

OpenSSH (OpenBSD Secure Shell) 是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。

本周，OpenSSH 修补了上述产品存在安全漏洞，避免攻击者利用漏洞发起拒绝服务攻击。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/61980>

本周要闻速递

1. 安卓曝无限重启漏洞 (CVE-2015-3823)

安全研究员们发现了一个安卓安全漏洞，他们声称可以让你的安卓手机无响应而且无限重启——该漏洞编号为 CVE-2015-3823，黑客利用它可以让安卓手机无限重启，这听起来有点像 Stagefright 漏洞，它源于媒体服务器 (mediaserver) 内置程序设计不当。由于近 90% 的安卓用户运行的系统是 4.0.1 到 5.1.1 版本，所以很不幸，这个漏洞杀伤力很强。

参考链接：<http://www.freebuf.com/news/74261.html>

2. Mac 平台新型蠕虫病毒曝光

两名研究人员开发出第一个可感染 Mac 的固件蠕虫病毒，并且可以在无需联网的情况下在 MacBook 间进行自动传播。该病毒被称为 “Thunderstrike 2”，是年初 “Thunderstrike” 病毒的变种 (FreeBuf 曾详细报道过)。它可以在固件层面感染 Mac，并且难以根除。固件被感染后将不能进行修复或升级，这意味着人们几乎对它束手无策。漏洞作者仍为 LegbaCore 公司创始人、安全专家 Trammell Hudso，他也是另一种 BIOS 恶意软件 Xeno Kovah 的创造者。Thunderstrike 展示了蠕虫通过外设 (Thunderbolt 接口) 物理接触及利用苹果 EFI 安全漏洞恶意传播的能力，而 Thunderstrike 2 则拥有通过恶意网站或电邮即可传播的能力。

参考链接：<http://www.freebuf.com/news/74216.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