

信息安全漏洞周报

2015 年 02 月 16 日-2015 年 03 月 01 日

2015 年第 8、9 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 175 个，其中高危漏洞 33 个、中危漏洞 126 个、低危漏洞 16 个。上述漏洞中，可利用来实施远程攻击的漏洞有 159 个。本周收录的漏洞中，已有 152 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“Zeus cart 存在多个漏洞”、“Maarch LetterBox 任意文件上传漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。本周，UNIX/Linux 系统中应用广泛的 Samba 组件被披露存在高危远程代码执行漏洞，请 UNIX/Linux 系统管理员注意加强防范。

成员单位报送漏洞统计

本周，共 6 家成员单位及个人报送了本周收录的全部 175 个漏洞。报送情况如表 1 所示。其中，奇虎 360、天融信、启明星辰、绿盟科技、恒安嘉新等单位报送数量较多。此外，补天平台、CNCERT 各分中心及白帽子向 CNVD 提交了 1166 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	1140	1140
天融信	169	0
启明星辰	156	0
绿盟科技	108	0
恒安嘉新	101	0
安天实验室	46	0

东软	1	0
CNCERT 江西分中心	9	9
CNCERT 山西分中心	4	4
CNCERT 宁夏分中心	4	4
CNCERT 河南分中心	3	3
个人	6	6
报送总计	1747	1166
录入总计	175（去重）	1166

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、IBM、Cisco 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	Mozilla	19	11%
2	IBM	15	9%
3	Cisco	11	6%
4	WordPress	10	6%
5	Drupal	7	4%
6	Moodle	7	4%
7	McAfee	5	3%
8	SAP	5	3%
9	Siemens	5	3%
10	其他	91	51%

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 175 个漏洞。其中应用程序漏洞 123 个，WEB 应用漏洞 34 个，网络设备漏洞 10 个，操作系统漏洞 7 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	123
WEB 应用漏洞	34
网络设备漏洞	10
操作系统漏洞	7
安全产品漏洞	1

表 3 漏洞按影响类型统计表

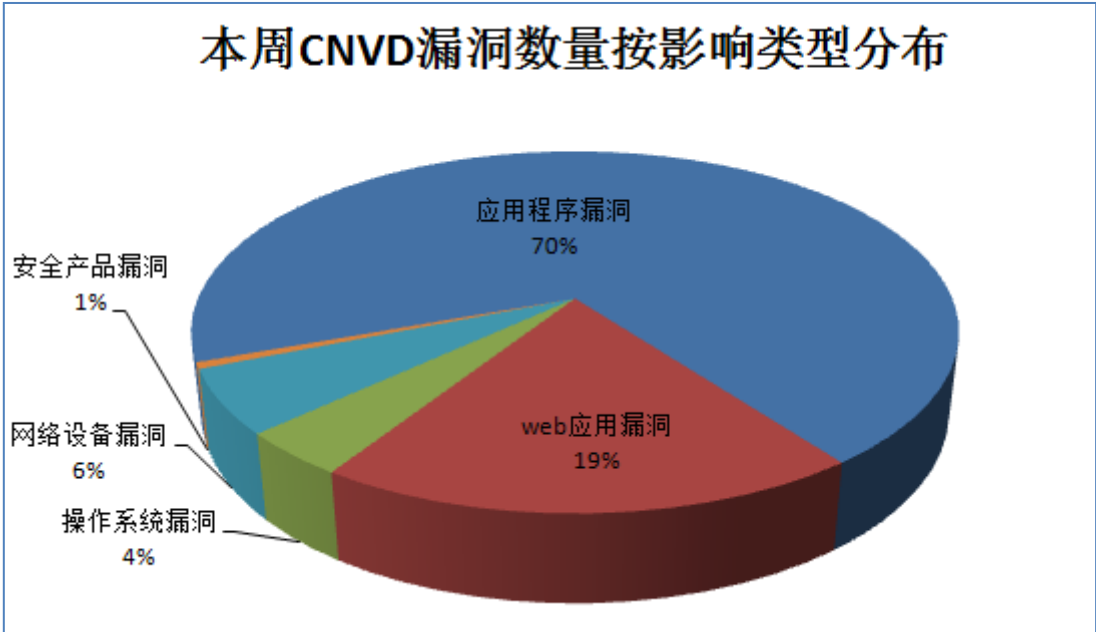


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 12 个电信行业漏洞，3 个移动互联网行业漏洞，6 个工控系统行业漏洞（如下图表所示）。其中，“IBM Tivoli Storage Manager 竞争条件权限提升漏洞、IBM Tivoli Storage Manager 权限提升漏洞、Motorola Mobility Scanner SDK 本地特权提升漏洞、Android 整数溢出漏洞、Advantech EKI-1200 Series 存在未明缓冲区溢出漏洞”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-2015-01177	IBM Tivoli Storage Manager 竞争条件权限提升漏洞	高	是
电信	CNVD-2015-01178	IBM Tivoli Storage Manager 权限提升漏洞	高	是
电信	CNVD-2015-01221	Cisco ASR 5000 Series Software 拒绝服务漏洞	中	是
电信	CNVD-2015-01251	IBM Tivoli Storage Manager 本地信息泄露漏洞	低	是
电信	CNVD-2015-01271	IBM WebSphere MQ 资源管理拒绝服务	低	是

		漏洞		
电信	CNVD-2015-01273	IBM WebSphere Portal 跨站脚本漏洞 (CNVD-2015-01273)	低	是
电信	CNVD-2015-01266	Motorola Mobility Scanner SDK 存在多个栈缓冲区溢出漏洞	中	是
电信	CNVD-2015-01265	Motorola Mobility Scanner SDK 本地特权提升漏洞	高	是
电信	CNVD-2015-01336	IBM Tivoli Endpoint Manager Web Reports 组件跨站脚本漏洞	中	是
电信	CNVD-2015-01332	D-Link DIR-645 存在多个漏洞	中	否
电信	CNVD-2015-01326	ISC BIND 远程拒绝服务漏洞 (CNVD-2015-01326)	中	是
电信	CNVD-2015-01321	多个 NetGear Routers SOAP 服务验证绕过漏洞	中	否
移动互联网	CNVD-2015-01258	Android 整数溢出漏洞	高	是
移动互联网	CNVD-2015-01294	Android 'GraphicBuffer::unflatten'函数整数溢出漏洞	中	是
移动互联网	CNVD-2015-01335	Google Email Application for Android 拒绝服务漏洞	中	是
工控系统	CNVD-2015-01199	Siemens SIMATIC STEP 7 敏感信息泄露漏洞	低	是
工控系统	CNVD-2015-01196	Siemens SIMATIC STEP 7 TIA Portal 中间人攻击信息泄露漏洞	中	是
工控系统	CNVD-2015-01197	Siemens SIMATIC STEP 7 TIA Portal 密码哈希算法安全漏洞	低	是
工控系统	CNVD-2015-01198	Siemens SIMATIC STEP 7 安全绕过漏洞	中	是
工控系统	CNVD-2015-01247	Advantech EKI-1200 Series 存在未明缓冲区溢出漏洞	高	是
工控系统	CNVD-2015-01296	Siemens SIMATIC WinCC TIA Portal 中间人信息泄露漏洞	中	是

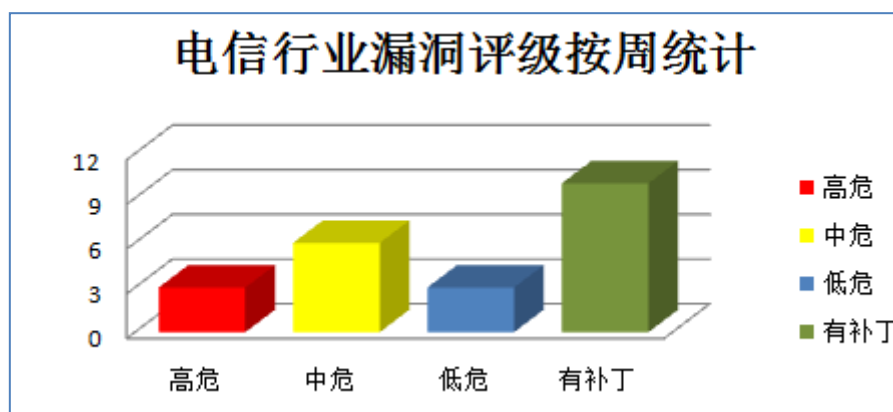


图1 电信行业漏洞统计

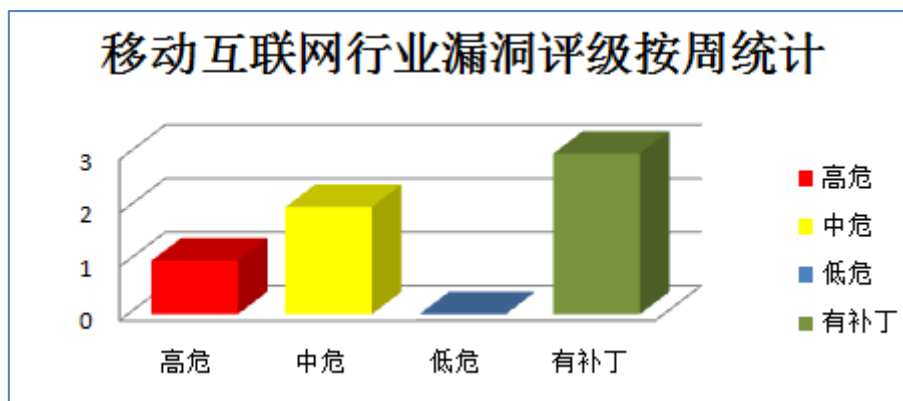


图 2 移动互联网行业漏洞统计

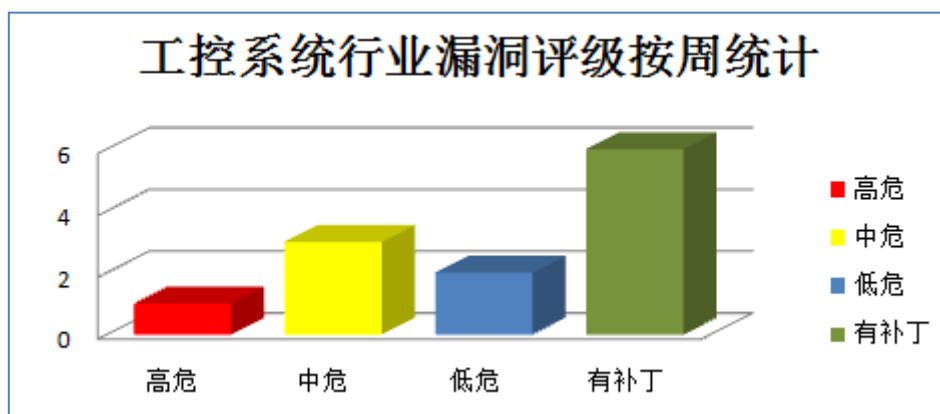


图 3 工控系统行业漏洞统计

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、Samba 产品安全漏洞

2 月 25 日，CNVD 收录了 Samba 组件存在的一个任意代码执行漏洞（CNVD-2015-01174，对应 CVE-2015-0240）。由于 Samba 组件广泛应用于 Linux 和 UNIX 系统，致使主流 GNU/Linux 发行版都受到了影响。攻击者成功利用漏洞可以当前用户权限远程执行代码，导致 Samba 服务崩溃或控制操作系统主机。

CNVD 收录的相关漏洞包括：Samba 任意代码执行漏洞。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-2015-01174>

2、Mozilla 产品安全漏洞

Mozilla Firefox/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/邮件客户端。本周，上述产品被披露存在信息泄露、内存破坏、缓冲区溢出和拒绝服务漏洞，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：Mozilla Firefox/Thunderbird 存在未明内存破坏漏洞(CNVD-2015-01287、CNVD-2015-01293)、Mozilla Firefox 错误引用拒绝服务漏洞、Mozilla Firefox 缓冲区溢出漏洞(CNVD-2015-01286)、Mozilla Firefox 中间人信息泄露漏洞、Mozilla Firefox 内存破坏漏洞 (CNVD-2015-01289)、Mozilla Firefox 拒绝服务漏洞 (CNVD-2015-01290)、Mozilla Firefox/Thunderbird 拒绝服务漏洞 (CNVD-2015-01291)。其中“Mozilla Firefox/Thunderbird 存在未明内存破坏漏洞 (CNVD-2015-01287、CNVD-2015-01293)、Mozilla Firefox 错误引用拒绝服务漏洞”漏洞的综合评级均为“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-2015-01287>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01293>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01190>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01286>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01288>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01289>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01290>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01291>

3、Moodle 产品安全漏洞

Moodle 是一款开放源代码的网络教学应用程序。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发起拒绝服务。

CNVD 收录的相关漏洞包括：Moodle 跨站脚本漏洞、Moodle Glossary 跨站请求伪造漏洞、Moodle 信息泄露漏洞、Moodle 'calendar/externallib.php'信息泄露漏洞、Moodle multimedia 过滤器拒绝服务漏洞、Moodle Shibboleth 验证插件强制退出漏洞、Moodle LTI 模块不充分访问检查漏洞。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-2015-01226>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01227>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01228>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01229>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01230>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01231>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01232>

4、Linux kernel 产品安全漏洞

Linux kernel 是一款开源的操作系统。本周，上述产品被披露存在缓冲区溢出漏洞等多个漏洞，攻击者可利用漏洞提升权限、使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Linux Kernel ASLR 整数溢出漏洞、Linux Kernel ASLR 实现不充分漏洞、Linux Kernel 'fs/ecryptfs/crypto.c'本地缓冲区溢出漏洞。目前，除“Linux Kernel ASLR 整数溢出漏洞”外，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-2015-01315>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01316>

5、HumHub '.htaccess'任意文件上传漏洞

HumHub 是一个灵活，开源的社交网络系统。本周，HumHub 被披露存在综合评级为“高危”的任意文件上传漏洞。攻击者可以利用漏洞上传任意文件并执行。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-2015-01309>

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-2015-01201	WordPress 插件 WP Slimstat 弱加密漏洞	高	用户可以联系供应商获得补丁信息： https://wordpress.org/
CNVD-2015-01209	Drupal Avatar Uploader 任意文件上传漏洞	高	Avatar Uploader 6.x-1.3 已经修复该漏洞，建议用户下载更新： http://drupal.org/
CNVD-2015-01216	GNU glibc 'strxfrm()'函数整数溢出漏洞	高	暂无
CNVD-2015-01233	GNU glibc 'strcoll()'函数栈缓冲区溢出漏洞	高	暂无
CNVD-2015-01225	WordPress Image Metadata Cruncher 跨站请求和 HTML 注入漏洞	高	暂无
CNVD-2015-01224	WordPress Photo Gallery 插件任意文件上传漏洞	高	暂无
CNVD-2015-01247	Advantech EKI-1200 Series 存在未明缓冲区溢出漏洞	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://support.advantech.com.tw/Support/DownloadSRDetail_New.aspx?SR_ID=1-V6XOHK&Doc_Source=

			Download
CNVD-2015-01276	McAfee Data Loss Prevention Endpoint SQL 注入漏洞 (CNVD-2015-01276)	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://kc.mcafee.com/corporate/index?page=content&id=SB10098
CNVD-2015-01282	Persistent Systems Radia Client Automation 代码注入漏洞	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： https://radiasupport.accelerite.com/hc/en-us/articles/203659814-Accelerite-releases-solutions-and-best-practices-to-enhance-the-security-for-RBAC-and-Remote-Notify-features
CNVD-2015-01280	Lexmark Markvision Enterprise LibraryFileUploadServlet servlet 目录遍历漏洞	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://support.lexmark.com/index?page=content&id=TE677&locale=EN&userlocale=EN_US

表 3 部分高危漏洞列表

小结：2月25日，CNVD收录了Samba组件存在的一个任意代码执行漏洞，攻击者成功利用漏洞可以当前用户权限远程执行代码，导致Samba服务崩溃或控制操作系统主机。此外，Mozilla、Moodle多款产品及Linux kernel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、进行跨站攻击、提升权限、执行任意代码或发起拒绝服务攻击。另外，HumHub被批露存在一个高危零日漏洞，攻击者可利用漏洞上传任意文件并执行。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、Apple 修补 CUPS 产品漏洞

Apple CUPS 是美国苹果（Apple）公司的一套开源的用于 OS X 和类 Unix 系统的打印系统。该系统基于 Internet 打印协议（IPP），提供大多数 PostScript 和 raster 打印机服务。

本周，Apple 修补了上述产品存在的缓冲区溢出漏洞，避免攻击者利用漏洞提交特殊请求使应用程序崩溃或执行任意代码。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/55523>

本周要闻速递

1. Uber 数据库遭入侵，50000 名司机信息泄露

著名打车应用 Uber 今日发布公告，称其数据库遭到第三方黑客入侵，50000 名司机的信息泄露，包括司机姓名和驾驶证号。这次入侵发生在 2014 年 5 月 13 日，Uber 于 9 月发现（响应有点慢啊……）后立即开始调查，但是 Uber 并没有解释为何拖了这么久才公开这次安全事件。为了赔偿受到影响的司机，Uber 称将提供免费一年的 Experian 公司（一家知名信息服务公司）账户保护服务，漏洞事件还报告给了加州总检察长办公室，但目前未得到后者的回应。除此之外，Uber 还想通过法律途径找到那位入侵的第三方。

参考链接：<http://www.freebuf.com/news/59626.html>

2. WordPress 流量统计插件 Slimstat 存在高危漏洞

WordPress 最流行的插件之一、网站流量实时统计插件 WP-Slimstat 被曝存在高危漏洞，影响全球 100 万以上网站。WP-Slimstat 全称为 Wettable Powder Slimstat，是 WordPress 上最流行的网站流量实时统计插件。全球共有 7000 万使用 WordPress 搭建的网站，其中有超过 130 万使用了 WP-Slimstat 这款插件。所有 3.9.6 以前版本的 WP-Slimstat 都包含一个简单可猜测的密钥，这个密钥被 WP-Slimstat 用来标记网站的访问者。只要该密钥被攻破，攻击者可以通过 SQL 注入（盲注）攻击目标网站以获取敏感的数据库信息，包括用户名、密码（hash）以及至关重要的 wordpress 安全密钥。

参考链接：<http://www.freebuf.com/news/59443.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