

信息安全漏洞周报

2015 年 11 月 2 日-2015 年 11 月 8 日

2015 年第 45 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 200 个，其中高危漏洞 53 个、中危漏洞 131 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 169 个。本周收录的漏洞中，已有 153 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“WordPress wp-championship 插件 SQL 注入漏洞”、“Zhone Technologies zNID GPON 远程代码执行漏洞”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 8 家成员单位、合作伙伴及个人报送了本周收录的全部 200 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、启明星辰、安天实验室、绿盟科技等单位报送数量较多。补天平台、乌云、漏洞盒子及白帽子向 CNVD 提交了 614 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(补天平台)	281	281
启明星辰	158	0
安天实验室	158	0
绿盟科技	116	0
天融信	82	0
恒安嘉新	22	0

H3C	9	0
知道创宇	1	0
乌云	291	291
漏洞盒子	4	4
CNCERT 甘肃分中心	4	4
个人	34	34
报送总计	5683	614
录入总计	200（去重）	614

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Apple、Kaspersky、Drupal 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	Apple	34	17%
2	Kaspersky	10	5%
3	Drupal	8	4%
4	Janitza	7	4%
5	Infinite Automation Systems, Inc.	7	4%
6	Samsung	6	3%
7	Apache	5	3%
8	NTP	5	3%
9	Lenovo	5	3%
10	其他	113	54%

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 200 个漏洞。其中应用程序漏洞 114 个，操作系统漏洞 37 个，Web 应用漏洞 27 个，网络设备漏洞 11 个，安全产品漏洞 11 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	114

操作系统漏洞	37
Web 应用漏洞	27
网络设备漏洞	11
安全产品漏洞	11

表 3 漏洞按影响类型统计表

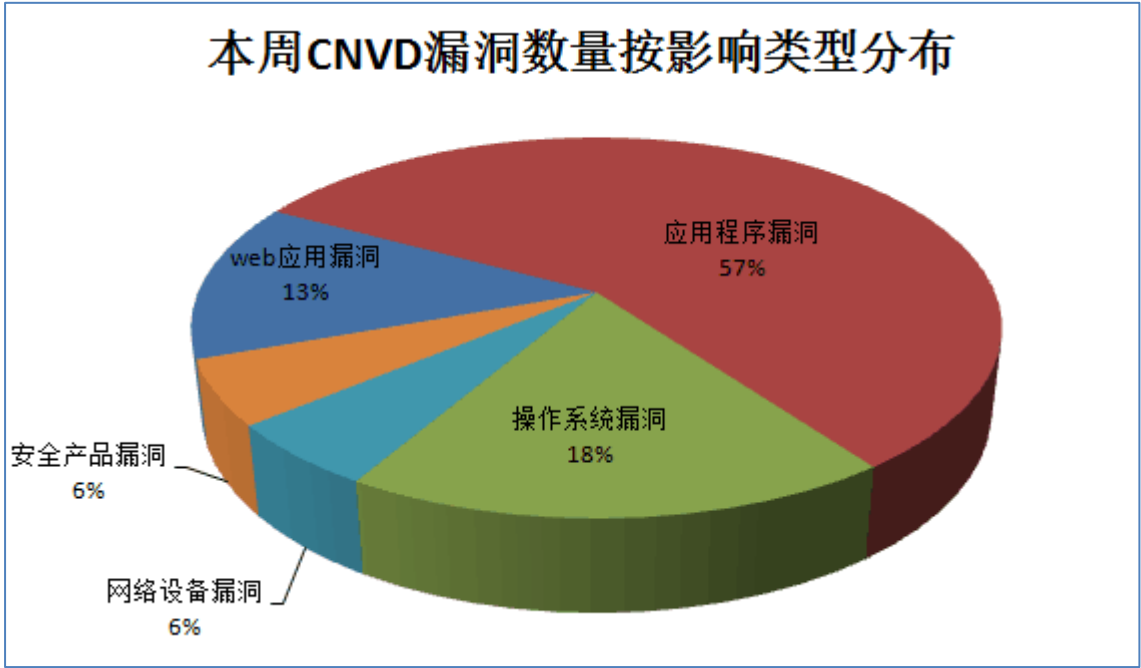


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 6 个电信行业漏洞、31 个移动互联网行业漏洞、13 个工系统行业漏洞（如下图表所示）。其中，“Apple OS X Script Editor 限制绕过漏洞、Apple iOS 任意代码执行漏洞、Apple iOS 双重释放漏洞、Apple iOS 任意代码执行漏洞（CNVD-2015-07162）、Apple iOS/Safari/iTunes 内存破坏漏洞（CNVD-2015-07152）、Apple iOS/OS X Dish Images 内存破坏漏洞（CNVD-2015-07156）、Qolsys IQ Panel 安全绕过漏洞、Qolsys IQ Panel 使用硬编码加密密钥漏洞、Android mediaserver 远程代码执行漏洞、Android mediaserver 内存破坏漏洞”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-2015-07251	MiniUPnP Client 缓冲区溢出漏洞	中	是
电信	CNVD-2015-07261	Zhone Technologies zNID GPON 身份验证绕过漏洞	中	否
电信	CNVD-2015-07264	Zhone Technologies zNID GPON 远程代	高	否

		码执行漏洞		
电信	CNVD-2015-07265	Zhone Technologies zNID GPON 信息泄露漏洞	高	否
电信	CNVD-2015-07308	IBM WebSphere Portal 信息泄露漏洞 (CNVD-2015-07308)	中	是
电信	CNVD-2015-07309	Cisco ASR 5000 设备拒绝服务漏洞	中	是
移动互联网	CNVD-2015-07136	Apple OS X Script Editor 限制绕过漏洞	高	是
移动互联网	CNVD-2015-07148	Apple iOS 拒绝服务漏洞 (CNVD-2015-07148)	中	是
移动互联网	CNVD-2015-07147	Apple iOS 拒绝服务漏洞 (CNVD-2015-07147)	中	是
移动互联网	CNVD-2015-07146	Apple iOS 拒绝服务漏洞 (CNVD-2015-07146)	中	是
移动互联网	CNVD-2015-07145	Apple iOS 任意代码执行漏洞	高	是
移动互联网	CNVD-2015-07144	Apple iOS 双重释放漏洞	高	是
移动互联网	CNVD-2015-07143	Apple iOS 拒绝服务漏洞 (CNVD-2015-07143)	中	是
移动互联网	CNVD-2015-07142	Apple iOS 拒绝服务漏洞 (CNVD-2015-07142)	中	是
移动互联网	CNVD-2015-07141	Apple iOS 拒绝服务漏洞 (CNVD-2015-07141)	中	是
移动互联网	CNVD-2015-07162	Apple iOS 任意代码执行漏洞 (CNVD-2015-07162)	高	是
移动互联网	CNVD-2015-07152	Apple iOS/Safari/iTunes 内存破坏漏洞 (CNVD-2015-07152)	高	是
移动互联网	CNVD-2015-07161	Apple iOS CFNetwork cookie 改写漏洞	中	是
移动互联网	CNVD-2015-07160	Apple iOS/OS X/watchOS 堆缓冲区溢出漏洞	中	是
移动互联网	CNVD-2015-07151	Apple iOS/Safari/iTunes 内存破坏漏洞 (CNVD-2015-07151)	中	是
移动互联网	CNVD-2015-07150	Apple iOS/Safari/iTunes 内存破坏漏洞 (CNVD-2015-07150)	中	是
移动互联网	CNVD-2015-07154	Apple Safari/iTunes 内存破坏漏洞 (CNVD-2015-07154)	中	是
移动互联网	CNVD-2015-07159	Apple iOS BOM 目录遍历漏洞	中	是
移动互联网	CNVD-2015-07149	Apple iOS/Safari/iTunes 内存破坏漏洞 (CNVD-2015-07149)	中	是
移动互联网	CNVD-2015-07158	Apple iOS/OS X/watchOS 内存破坏漏洞 (CNVD-2015-07158)	中	是
移动互联网	CNVD-2015-07157	Apple iOS/OS X Dish Images 内存破坏漏洞 (CNVD-2015-07157)	中	是
移动互联网	CNVD-2015-07156	Apple iOS/OS X Dish Images 内存破坏漏洞 (CNVD-2015-07156)	高	是

移动互联网	CNVD-2015-07153	Apple iOS/OS X FontParser 内存破坏漏洞（CNVD-2015-07153）	中	是
移动互联网	CNVD-2015-07163	Apple iOS 内存破坏漏洞（CNVD-2015-07163）	中	是
移动互联网	CNVD-2015-07193	Android ‘PPP Character Device Driver’本地拒绝服务漏洞	低	否
移动互联网	CNVD-2015-07199	Qolsys IQ Panel 安全绕过漏洞	高	是
移动互联网	CNVD-2015-07198	Qolsys IQ Panel 使用硬编码加密密钥漏洞	高	是
移动互联网	CNVD-2015-07217	百度 Moplus SDK 存在设计漏洞(WormHole 漏洞)	高	否
移动互联网	CNVD-2015-07235	Android mediaserver 远程代码执行漏洞	高	是
移动互联网	CNVD-2015-07234	Android mediaserver 内存破坏漏洞	高	是
移动互联网	CNVD-2015-07233	Android mediaserver 信息泄露漏洞	中	是
移动互联网	CNVD-2015-07277	Apple WebKit 拒绝服务漏洞	中	是
工控系统	CNVD-2015-07173	Infinite Automation Mango Automation 文件上传漏洞	中	否
工控系统	CNVD-2015-07172	Infinite Automation Mango Automation SQL 注入漏洞	中	否
工控系统	CNVD-2015-07171	Infinite Automation Mango Automation 信息泄露漏洞（CNVD-2015-07171）	中	否
工控系统	CNVD-2015-07170	Infinite Automation Mango Automation 任意命令执行漏洞	中	否
工控系统	CNVD-2015-07169	Infinite Automation Mango Automation 信息泄露漏洞（CNVD-2015-07169）	中	否
工控系统	CNVD-2015-07168	Infinite Automation Mango Automation 跨站脚本漏洞	低	否
工控系统	CNVD-2015-07167	Infinite Automation Mango Automation 跨站请求伪造漏洞	中	否
工控系统	CNVD-2015-07268	SDG Technologies Plug 和 Play SCADA 跨站脚本漏洞	中	否
工控系统	CNVD-2015-07306	Allen-Bradley MicroLogix 拒绝服务漏洞	高	否
工控系统	CNVD-2015-07305	Allen-Bradley MicroLogix 任意文件插入漏洞	中	否
工控系统	CNVD-2015-07304	Allen-Bradley MicroLogix 堆栈缓冲区溢出漏洞	高	否
工控系统	CNVD-2015-07303	Allen-Bradley MicroLogix 跨站脚本漏洞	中	否
工控系统	CNVD-2015-07307	Allen-Bradley MicroLogix SQL 注入漏洞	中	否

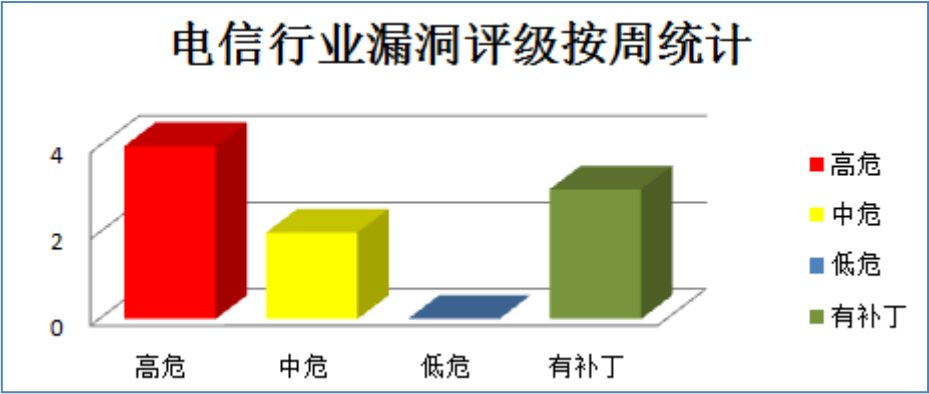


图 1 电信行业漏洞统计

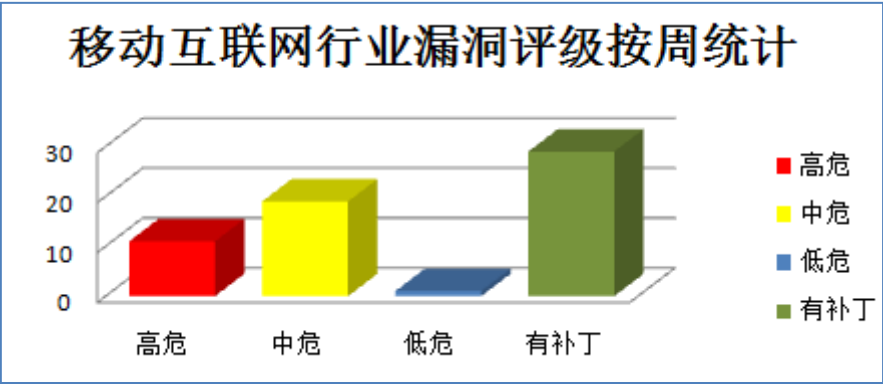


图 2 移动互联网行业漏洞统计

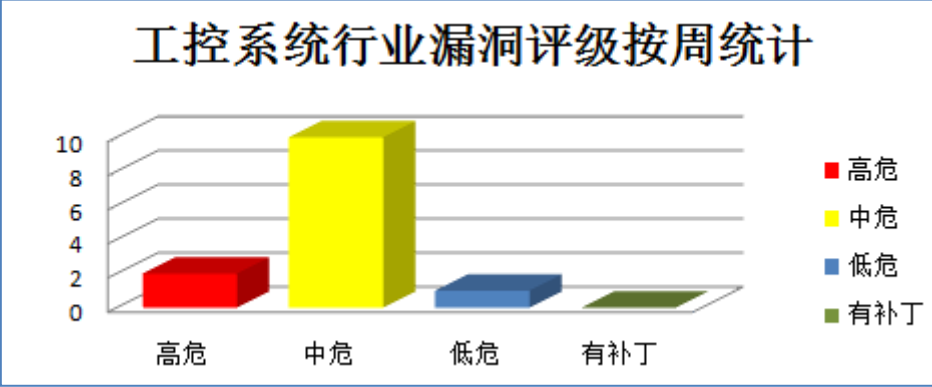


图 3 工控系统行业漏洞统计

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、Apple 操作系统安全漏洞

OS X(前称 Mac OS X)OS X 是苹果公司为 Mac 系列产品开发的专属操作系统；iOS 是由苹果公司为移动设备所开发的操作系统。本周，上述产品存在多个漏洞。远程攻击者可利用漏洞执行任意代码及任意文件写入、提升权限和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apple iOS 双重释放漏洞、Apple OS X 符号链接攻

击漏洞、Apple iOS 任意代码执行漏洞、Apple iOS/OS X Disk Images 内存破坏漏洞 (CNVD-2015-07156)、Apple OS X Script Editor 限制绕过漏洞、Apple OS X 权限提升漏洞、Apple OS X Graphics Drivers 内存破坏漏洞、Apple iOS/Safari/iTunes 内存破坏漏洞 (CNVD-2015-07152)。上述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-2015-07144>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07133>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07145>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07156>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07136>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07137>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07140>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07152>

2、Cisco 产品安全漏洞

Cisco FireSIGHT Management Center (MC) 是一套集中对 Cisco ASA with FirePOWER Services 和 Cisco FirePOWER 网络安全设备进行管理的管理中心软件；Cisco ASR 5500 System Architecture Evolution (SAE) Gateway 是一款 Cisco ASR 5000 系列移动多媒体服务解决方案网关产品；Cisco Secure Access Control Server (ACS) 是一款安全访问控制服务器，Solution Engine 是其中的一个服务器引擎解决方案；Cisco Unified Border Element 是一个智能统一通信网络边界组件；Cisco FireSight 管理中心是一款整体可视性安全管理平台，此安全管理控制台和数据存储库产品可为用户实现安全运营提供集中的事件和策略管理；Cisco Prime Service Catalog 是美国思科公司推出的通过一个单一的门户网站提供的所有服务的解决方案。本周，上述产品存在多个漏洞，远程攻击者可利用漏洞，执行任意 SQL 指令、注入任意 Web 脚本或 HTML 和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco FireSight Management Center 跨站脚本漏洞、Cisco ASR 5500 SAE 网关拒绝服务漏洞、Cisco ACS Solution Engine 跨站脚本漏洞、Cisco Unified Border Element 拒绝服务漏洞、多款 Cisco FireSight 管理中心跨站脚本漏洞、Cisco Prime Service Catalog WEB 框架 SQL 注入漏洞、Cisco ASR 5000 设备拒绝服务漏洞。目前，厂商已经发布了“Cisco FireSight Management Center 跨站脚本漏洞、Cisco ASR 5500 SAE 网关拒绝服务漏洞、Cisco Unified Border Element 拒绝服务漏洞、Cisco ASR 5000 设备拒绝服务漏洞”的漏洞修补程序。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-2015-07246>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07232>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07231>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07197>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07200>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07196>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07309>

3、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。其中，Overlay 是其中的一个能够在网页的顶层显示 Drupal 管理界面的模块；Entity Registration 是其中的一个用户登记注册模块；Stickynote 是其中的一个基于路径对页面进行注解的模块；Taxonomy Find 是其中的一个提供了搜索界面的分类查找模块；User Dashboard 是其中的一个仪表板模块；Twilio 是其中的一个通信模块；Webform CiviCRM Integration 是其中的一个将 Webform 和 CiviCRM 进行整合的模块。本周，上述产品模块存在多个漏洞，远程攻击者可利用漏洞，获取敏感信息、执行未经授权操作或执行钓鱼等其他攻击。

CNVD 收录的相关漏洞包括：Drupal core Overlay 模块开放重定向漏洞、Drupal Entity Registration 模块信息泄露漏洞、Drupal Stickynote 模块跨站脚本漏洞（CNVD-2015-07318）、Drupal Taxonomy Find 模块存在未明漏洞、Drupal User Dashboard 模块 SQL 注入漏洞、Drupal Twilio 模块访问绕过漏洞、Drupal Webform CiviCRM Integration 模块跨站脚本漏洞、Drupal ‘web-fixtures\issue130.php’ 跨站脚本漏洞。其中，“Drupal User Dashboard 模块 SQL 注入漏洞”漏洞的综合评级为“高危”。除“Drupal Taxonomy Find 模块存在未明漏洞、Drupal ‘web-fixtures\issue130.php’ 跨站脚本漏洞”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-2015-07316>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07319>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07318>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07317>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07320>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07185>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07184>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07186>

4、IBM 产品安全漏洞

IBM WebSphere Portal 是一套企业门户软件，该软件能够创建一个联接企业内部和外部的平台，可让员工、客户和供应商等通过该平台访问企业内部数据；IBM Domino

是一套用于托管社交商务应用的平台，该平台将业务消息传递、应用和社交协作结合在一起，并为用户提供实时在线交流功能；IBM QRadar Security Information and Event Manager 是一套可对分散在整个网络中的数千个设备和应用中的日志源事件数据进行整合的解决方案。本周，上述产品存在多个漏洞。远程攻击者可利用漏洞，执行任意代码、提升权限或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM WebSphere Portal 访问绕过漏洞、IBM Domino SMTP 缓冲区溢出漏洞、IBM Domino 缓冲区溢出漏洞、IBM WebSphere Portal 信息泄露漏洞（CNVD-2015-07308）、IBM QRadar Security Information and Event Manager 权限提升漏洞。其中，“IBM Domino SMTP 缓冲区溢出漏洞、IBM Domino 缓冲区溢出漏洞、IBM QRadar Security Information and Event Manager 权限提升漏洞”的综合评级为“高危”。目前，厂商已发布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-2015-07213>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07214>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07210>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07308>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07203>

5、Samsung SmartViewer 远程代码执行漏洞

Samsung SmartViewer 是一套专为视频监控系统设计的视频查看软件。该软件支持通过互联网查看现场视频，以及搜索通过三星 DVR 或 NVR 连接的摄像头的视频。本周，Samsung SmartViewer 存在高危远程代码执行漏洞。攻击者利用该漏洞可构建特殊的 WEB 页，诱使用户解析，导致应用程序崩溃或执行任意代码。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-2015-07276>

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-2015-07166	Red Hat Enterprise Application Platform 拒绝服务漏洞	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://rhn.redhat.com/errata/RHSA-2015-1907.html
CNVD-2015-07175	Foxit Reader 和 Foxit PhantomPD F 内存破坏漏洞	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://www.foxitsoftware.com/products/pdf-reader/

CNVD-2015-07174	Foxit Reader 和 Foxit PhantomPD F 内存破坏漏洞 (CNVD-2015-07174)	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://www.foxitsoftware.com/products/pdf-reader/
CNVD-2015-07179	NTP 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://support.ntp.org/bin/view/Main/NtpBug2921
CNVD-2015-07192	lldp 'protocols/lldp.c'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://vincentbernat.github.io/lldpd/
CNVD-2015-07201	389 Directory Server nsSSL3Ciphers 首选项漏洞	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://fedorahosted.org/389/ticket/48194
CNVD-2015-07199	Qolsys IQ Panel 安全绕过漏洞	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.qolsys.com/
CNVD-2015-07198	Qolsys IQ Panel 使用硬编码加密密钥漏洞	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.qolsys.com/
CNVD-2015-07266	VMware ESXi 'SLPDPProcessMessage()'函数远程代码执行漏洞	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： http://www.vmware.com/
CNVD-2015-07212	GNU glibc 'LD_POINTER_GUARD'权限提升漏洞	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.gnu.org/software/libc/

表 3 部分高危漏洞列表

小结：本周，Apple 操作系统存在多个漏洞，远程攻击者可利用漏洞执行任意代码及任意文件写入、提升权限和发起拒绝服务攻击。此外，Cisco、Drupal、IBM 多款产品存在多个漏洞，远程攻击者可获取敏感信息、执行任意代码、提升权限、发起拒绝服务攻击或执行钓鱼等其他攻击。另外，Samsung SmartViewer 存在高危远程代码执行漏洞。攻击者利用该漏洞可构建特殊的 WEB 页，诱使用户解析，导致应用程序崩溃或执行任意代码。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、Linux 修补 Kernel 产品漏洞

Linux 是一种开源操作系统内核。

本周，Linux 修补了 Linux kernel 产品存在的本地安全绕过、堆内存破坏和拒绝服

务漏洞，允许攻击者利用漏洞绕过安全限制，执行未授权操作和发起拒绝服务攻击。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/66293>

<http://www.cnvd.org.cn/patchInfo/show/66292>

<http://www.cnvd.org.cn/patchInfo/show/66235>



本周要闻速递

1. vBulletin 5 曝远程命令执行漏洞，泄露大量数据

有报道指出 vBulletin 开发者网站遭遇黑客攻击并且泄露了将近 48 万 vBulletin 用户的敏感信息。在遭遇黑客攻击后，vBulletin 官方紧急强制性要求用户重置密码，他们警告用户：攻击者可能利用我们的系统漏洞得到了一些用户 ID 以及加密后的密码。随即，vBulletin 官网提及了一个用于连接 5.1.4 版本与 5.1.9 版本的安全补丁。此外，有黑客表示，已攻破了 vBulletin 官方网站并且得到了 479895 位用户的隐私信息，同时表示该漏洞还严重威胁到了福昕阅读器的论坛网站，并且该论坛已处于瘫痪状态。

参考链接：<http://www.freebuf.com/news/84024.html>

2. 谷歌自查安卓系统漏洞结果报告

据有关消息，谷歌团队尝试挑战“Android 的安全界限”，即在不和用户交流的前提下，远程获取到用户的通讯录、照片和信息；寻找源自 Google Play 下载，且未经用户允许的 app 中可以逃过检测直接安装到手机中的攻击软件。其中，研究人员最终发现，三星的代码中有 11 处安全漏洞。黑客可以借助这些漏洞制作具有系统特权的文件，窃取用户电子邮件，并在内核中执行代码，同时增加特权和非特权应用。

参考链接：<http://www.freebuf.com/news/84031.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