

信息安全漏洞周报

2014 年 12 月 15 日-2014 年 12 月 21 日

2014 年第 51 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 144 个，其中高危漏洞 41 个、中危漏洞 90 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 128 个。本周收录的漏洞中，已有 119 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“EntryPass N5200 Active Network Control Panel 信息泄露漏洞”、“Guruperl.net Advertise With Pleasure! Professional 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 144 个漏洞。报送情况如表 1 所示。其中，奇虎 360、天融信、安天实验室、绿盟科技、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、High-TechBridgeSecurity Research Lab 及白帽子向 CNVD 提交了 1246 个原创漏洞(注：奇虎 360 提交漏洞包含其“库带计划”中部分存量漏洞)。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	1217	1217
天融信	112	0
安天实验室	108	0
绿盟科技	105	0

恒安嘉新	80	0
启明星辰	61	0
High-Tech Bridge Security Research Lab	1	1
CNCERT 福建分中心	10	10
CNCERT 江西分中心	9	9
CNCERT 河南分中心	3	3
CNCERT 新疆分中心	1	1
CNCERT 山东分中心	1	1
个人	4	4
报送总计	1712	1246
录入总计	144（去重）	1246

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Drupal、Ettercap、Linux 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	Drupal	13	9%
2	Ettercap	8	6%
3	Linux	7	5%
4	Wordpress	6	4%
5	Schneider Electric	5	3%
6	Cisco	4	3%
7	ResourceSpace	4	3%
8	K7 Computing Pvt Ltd	3	2%
9	ManageEngine	3	2%
10	其他	91	63%

表 2 漏洞产品涉及厂商分布统计表

本周，CNVD 收录了 144 个漏洞。其中应用程序漏洞 93 个，WEB 应用漏洞 31 个，操作系统漏洞 8 个，网络设备漏洞 6 个，安全产品漏洞 5 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	93
WEB 应用漏洞	31
操作系统漏洞	8
网络设备漏洞	6
安全产品漏洞	5
数据库漏洞	1

表 3 漏洞按影响类型统计表

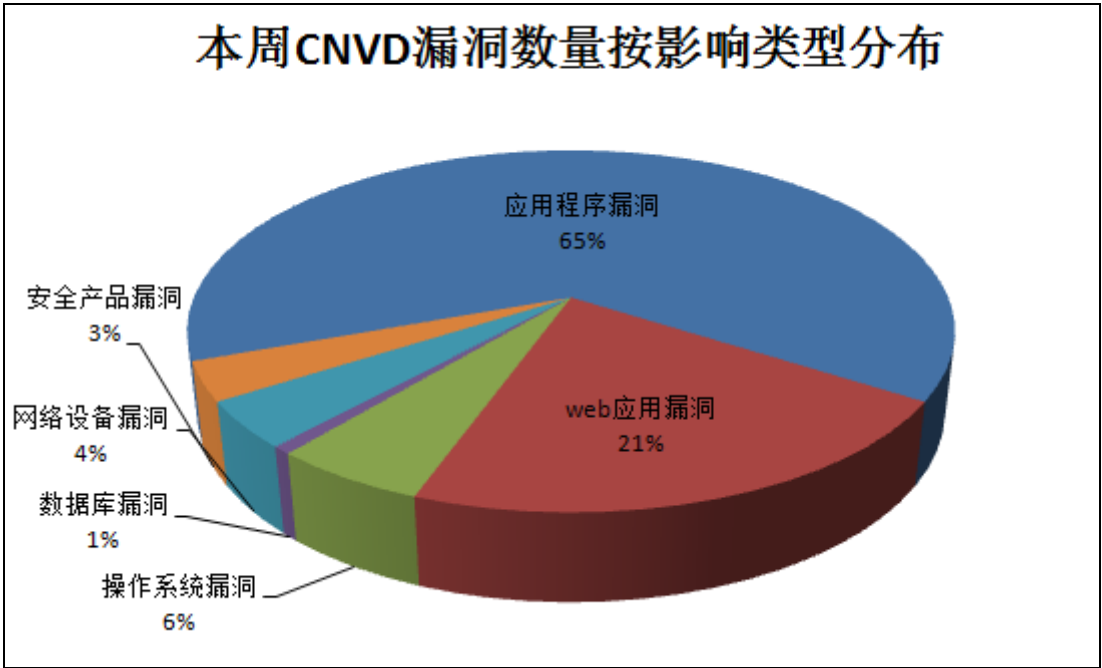


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 6 个电信行业漏洞， 1 个移动互联网行业漏洞（如下图表所示）。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2014-08965	Digicom DG-5514T ADSL 路由器权限提升漏洞	高	否
电信	CNVD-2014-08983	IBM WebSphere DataPower XC10 安全限制绕过漏洞	中	是
电信	CNVD-2014-08994	IBM WebSphere DataPower XC10 跨站请求伪造漏洞	中	是
电信	CNVD-2014-09002	ARRIS TG862G Route 跨站请求伪造漏洞	中	是

电信	CNVD-2014-09020	ARRIS TG862G 存在多个漏洞	中	是
电信	CNVD-2014-09033	Cisco IOS XR Software 拒绝服务漏洞 (CNVD-2014-09033)	中	是
移动互联网	CNVD-2014-08981	SQUARE ENIX Co. Ltd. Kaku-San-Sei Million Arthur for Android 权限提升漏洞	中	是

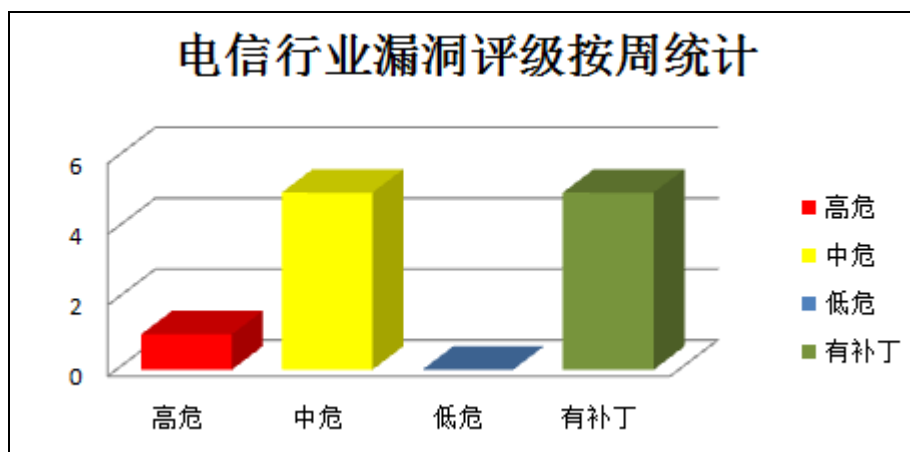


图 1 电信行业漏洞统计

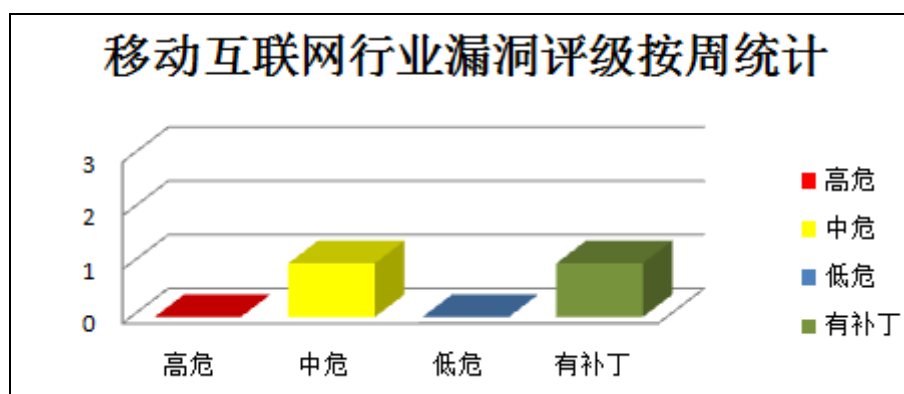


图 2 移动互联网行业漏洞统计

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、Schneider Electric 产品安全漏洞

施耐德电气为 100 多个国家的能源及基础设施、工业、数据中心及网络、楼宇和住宅市场提供整体解决方案。Schneider Electric ProClima 是热力计算软件。本周，上述产品被披露存在远程缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Schneider Electric ProClima 远程缓冲区溢出漏洞（CNVD-2014-09022、CNVD-2014-09023、CNVD-2014-09024、CNVD-2014-09025、CNV

D-2014-09017)。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-2014-09022>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09023>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09024>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09025>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09017>

2、Linux 产品安全漏洞

Linux Kernel 是 Linux 操作系统的内核。本周，上述产品被披露存在权限提升、拒绝服务和信息泄露漏洞，攻击者可利用漏洞提升权限、获取敏感信息或发起拒绝服务。

CNVD 收录的相关漏洞包括：Linux Kernel 'Polkit'本地权限提升漏洞、Linux Kernel 本地权限提升漏洞（CNVD-2014-09001）、Linux kernel MDP 驱动程序权限提升漏洞、Linux Kernel 'fs/isofs/rock.c'无限循环拒绝服务漏洞、Linux Kernel 'kernel/tls.c'本地信息泄露漏洞、Linux Kernel 'kernel/kvm.c'本地信息泄露漏洞。其中“Linux Kernel 'Polkit'本地权限提升漏洞、Linux Kernel 本地权限提升漏洞（CNVD-2014-09001）、Linux kernel MDP 驱动程序权限提升漏洞”的综合评级为“高危”。目前，除“Linux Kernel 'Polkit'本地权限提升漏洞”外，厂商已经发布了其余漏洞的修补程序。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-2014-09027>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09001>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08985>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09028>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08996>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09007>

3、FFmpeg 产品安全漏洞

FFmpeg 是一个免费的可以执行音讯和视讯多种格式的录影、转档、串流功能的软件。本周，上述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：FFmpeg 'libavcodec/mjpegdec.c'出界拒绝服务漏洞、FFmpeg 'libavcodec/pngdec.c'出界拒绝服务漏洞、FFmpeg 'libavcodec/rawdec.c'出界拒绝服务漏洞、FFmpeg 'libavcodec/hevc_ps.c'出界拒绝服务漏洞。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-2014-08971>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08970>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08969>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08968>

4、Cisco 产品安全漏洞

Cisco IOS 是多数思科系统路由器和网络交换机上使用的互连网络操作系统。Cisco Adaptive Security Appliance 是一款自适应安全设备，可提供安全和 VPN 服务的模块。Cisco ISB8320-E High-Definition IP-Only DVR 是思科的高清硬盘录像机。Cisco Prime Security Manager 是集中管理 Cisco ASA 5500-X 系列防火墙的工具。本周，上述产品被披露存在拒绝服务、跨站脚本和安全绕过漏洞，攻击者可利用漏洞进行跨站攻击、执行未授权操作或发起拒绝服务。

CNVD 收录的相关漏洞包括：Cisco IOS XR Software 拒绝服务漏洞（CNVD-2014-09033）、Cisco Adaptive Security Appliance 跨站脚本漏洞、Cisco ISB8320-E High-Definition IP-Only DVR 安全绕过漏洞、Cisco Prime Security Manager 存在多个跨站脚本漏洞。其中，“Cisco IOS XR Software 拒绝服务漏洞（CNVD-2014-09033）、Cisco Adaptive Security Appliance 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-2014-09033>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09032>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09026>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08986>

5、CMS Made Simple 存在未明 PHP 代码注入漏洞

CMS Made Simple (CMSMS) 是 CMSMS 团队开发的一套开源的内容管理系统(CMS)。本周，CMS Made Simple 被披露存在综合评级为“高危”的 PHP 代码注入漏洞。攻击者可以利用此漏洞注入 PHP 代码，并在受影响的应用程序中执行任意 PHP 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-2014-08989>

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-2014-08904	Lexmark MarkVision Enterprise 远程代码执行漏洞	高	用户可以联系供应商获得补丁信息： http://support.lexmark.com/index?page=productSelection&channel=supportAndDownloads&locale=zh&userlocale=ZH_CN
CNVD-2014-08905	MiniUPnP 存在多个漏洞	高	用户可以联系供应商获得补丁信息： http://miniupnp.free.fr/

CNVD-2014-08924	SAP SQL Anywhere 存在多个缓冲区溢出漏洞	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://scn.sap.com/docs/DOC-8218
CNVD-2014-09030	Morfy CMS 任意命令执行漏洞	高	暂无
CNVD-2014-08933	Plex Media Server web 服务器白名单绕过漏洞	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： https://forums.plex.tv/index.php/topic/62832-plex-media-server/?p=583250
CNVD-2014-08951	Intrex 存在未明任意文件上传漏洞	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://www.unitedplanet.com/en/intrex-6-professional
CNVD-2014-08964	GNU binutils 堆栈缓冲区溢出漏洞	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://gnu.april.org/software/binutils/binutils.html
CNVD-2014-08982	Montala ResourceSpace SQL 注入漏洞	高	暂无
CNVD-2014-08954	FreeType 'src/cff/cf2hints.c' 不完整修复远程栈缓冲区溢出漏洞	高	目前厂商已经发布升级补丁/版本以修复这个安全问题，请用户及时下载更新： http://www.freetype.org/
CNVD-2014-08955	Honeywell OPOS Suite 'HWOP OSSCANNER.ocx' 栈缓冲区溢出漏洞	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： https://www.honeywellaidc.com/en-us/Pages/default.aspx

表 3 部分高危漏洞列表

小结：本周，Schneider Electric 产品被批露存在远程缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码。另外，Linux、FFmpeg、Cisco 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞提升权限、获取敏感信息、进行跨站攻击、执行任意代码或发起拒绝服务。此外，CMS Made Simple 被披露存在一个高危零日漏洞。攻击者可以利用此漏洞注入 PHP 代码，并在受影响的应用程序中执行任意 PHP 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、Apache 修补 CloudStack/HTTP Server 产品漏洞

Apache CloudStack 是部署和管理大型虚拟机网络的开源软件。Apache HTTP Server 是 Apache 软件基金会的一个开放源码的网页服务器。

本周，Apache 修补了上述产品存在的身份验证绕过和拒绝服务漏洞，避免攻击者利用漏洞绕过身份验证或发起拒绝服务攻击。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/52950>

<http://www.cnvd.org.cn/patchInfo/show/52839>

本周要闻速递

1. 厄运 cookie（Misfortune Cookie）漏洞影响全球 1200 万台路由器

一个名为“厄运 cookie（Misfortune Cookie）”的严重漏洞正在影响全球 1200 万台路由器安全，D-Link、TP-Link、华为、中兴等品牌均受到影响，攻击者可以利用漏洞远程控制设备及监控流量。该漏洞与 AllegroSoft 公司开发的 WEB 服务器 RomPager 有关，RomPager 被诸多路由器厂商使用，嵌入路由设备固件以及调制调解器之中。这款 WEB 服务器可以为路由器提供良好用户体验的 Web 管理接口。

参考链接：<http://www.freebuf.com/news/54688.html>

2. Git 客户端中曝出高危漏洞

Git 官方近日发布一条重要消息，所有官方版本的 Git 客户端都存在高危漏洞，包括 GitHub Windows 和 Mac 客户端。因为该漏洞只存在于客户端中，所以 github.com 和 GitHub 企业版不会受到直接的影响。这个漏洞源于对大小写不敏感或者不区分大小写的文件系统。比如攻击者可以建立一个恶意的 Git 树使 git/config 被覆盖，从而修改 Git 仓库中的代码。Git 官方强烈建议所有 GitHub 用户和企业尽快更新客户端。同时如果用户访问代码副本托管在不安全或者不受信任主机上的 Git 库时，一定要格外小心。

参考链接：<http://www.freebuf.com/news/54658.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