

信息安全漏洞周报

2013 年 11 月 18 日-2013 年 11 月 24 日

2013 年第 47 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 135 个，其中高危漏洞 41 个、中危漏洞 79 个、低危漏洞 15 个。上述漏洞中，可利用来实施远程攻击的漏洞有 118 个。本周收录的漏洞中，已有 97 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“D-Link DSL-2740B 存在多个跨站请求伪造漏洞”、“MyBB Ajax forum stat Plugin 'ajaxfs.php' 存在多个 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、一家公司及个人报送了本周收录的全部 135 个漏洞。报送情况如表 1 所示。其中，启明星辰、天融信、绿盟科技等单位报送数量较多。此外，个人报送者向 CNVD 提交了 3 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	134	0
安天实验室	134	0
天融信	87	0
绿盟科技	51	0
恒安嘉新	20	0
知道创宇	1	0
深圳市深信服电子科技有限公司	1	0
个人	3	3

报送总计	431	3
录入总计	135（去重）	3

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 SAP、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	SAP	12	9%
2	IBM	7	5%
3	Cisco	6	4%
4	Linux	6	4%
5	LOCKON CO.LTD	6	4%
6	WordPress	5	4%
7	Mediawiki	5	4%
8	EMC	5	4%
9	Red Hat	1	1%
10	其它	82	61%

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 135 个漏洞。其中应用程序漏洞 92 个，WEB 应用漏洞 28 个，操作系统漏洞 10 个，网络设备漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	92
WEB 应用漏洞	28
网络设备漏洞	5
操作系统漏洞	10

表 3 漏洞按影响类型统计表

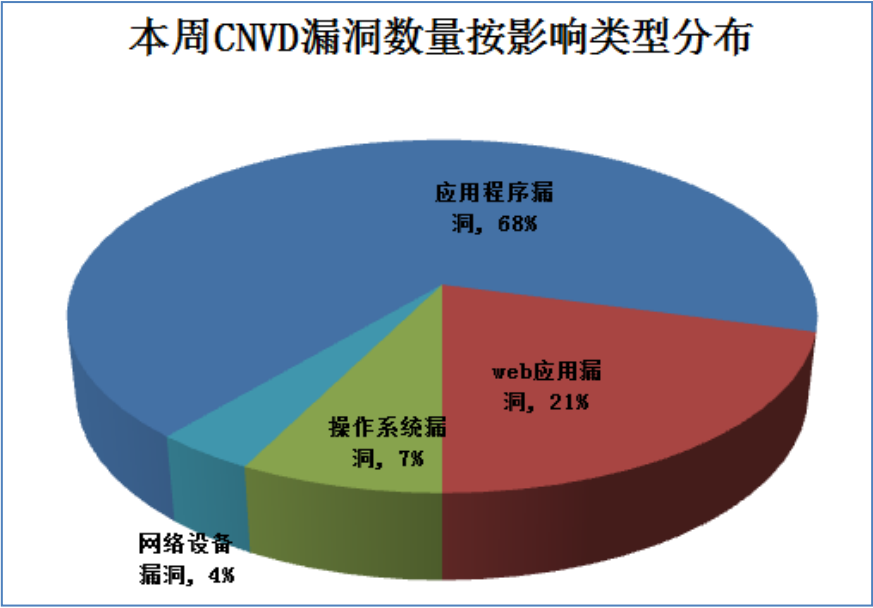


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 10 个电信行业漏洞、8 个移动互联网行业漏洞和 2 个工控系统漏洞（如下列表所示）。其中，“多个 Android Superuser Packages 任意命令执行漏洞、多个 Android Superuser 软件包任意命令执行漏洞、Catapult Software DNP3 Driver TCP 报文处理远程拒绝服务漏洞”的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-14599	D-Link DSL-2740B 存在多个跨站请求伪造漏洞	中	否
电信	CNVD-2013-14545	Samsung Galaxy S4 存在未明漏洞	中	否
电信	CNVD-2013-14549	IBM WebSphere Application Server 管理控制台存在未明反射型跨站脚本漏洞	低	是
电信	CNVD-2013-14550	IBM WebSphere Application Server 存在未明跨站脚本漏洞	中	是
电信	CNVD-2013-14551	IBM WebSphere Application Server 迁移角色分配权限提升漏洞	低	是
电信	CNVD-2013-14504	Cisco Unified Communications Manager Command-line Utility 本地安全绕过漏洞	中	是
电信	CNVD-2013-14505	Cisco Unified Communications	中	是

		Manager 目录遍历漏洞 (CNVD-2013-14505)		
电信	CNVD-2013-14509	Cisco Nexus 1000V 本地任意命令执行漏洞	中	是
电信	CNVD-2013-14518	Cisco IOS SSL VPN Interface 远程拒绝服务漏洞	中	是
电信	CNVD-2013-14516	IBM WebSphere Virtual Enterprise 跨站脚本漏洞	低	是
移动互联网	CNVD-2013-14638	BlackBerry Link 配置漏洞	中	是
移动互联网	CNVD-2013-14637	BlackBerry Link 远程文件访问功能权限提升漏洞	中	是
移动互联网	CNVD-2013-14569	多个 Android Superuser Packages 任意命令执行漏洞	高	是
移动互联网	CNVD-2013-14545	Samsung Galaxy S4 存在未明漏洞	中	否
移动互联网	CNVD-2013-14508	多个 Android Superuser 软件包搜索路径本地权限提升漏洞	中	否
移动互联网	CNVD-2013-14510	Apple iOS 本地安全绕过漏洞 (CNVD-2013-14510)	中	是
移动互联网	CNVD-2013-14511	Apple iOS Safari Mobile Web Browser 存在多个漏洞	中	否
移动互联网	CNVD-2013-14514	多个 Android Superuser 软件包任意命令执行漏洞	高	否
工控系统	CNVD-2013-14628	Catapult Software DNP3 Driver 本地拒绝服务漏洞	中	是
工控系统	CNVD-2013-14629	Catapult Software DNP3 Driver TCP 报文处理远程拒绝服务漏洞	高	是

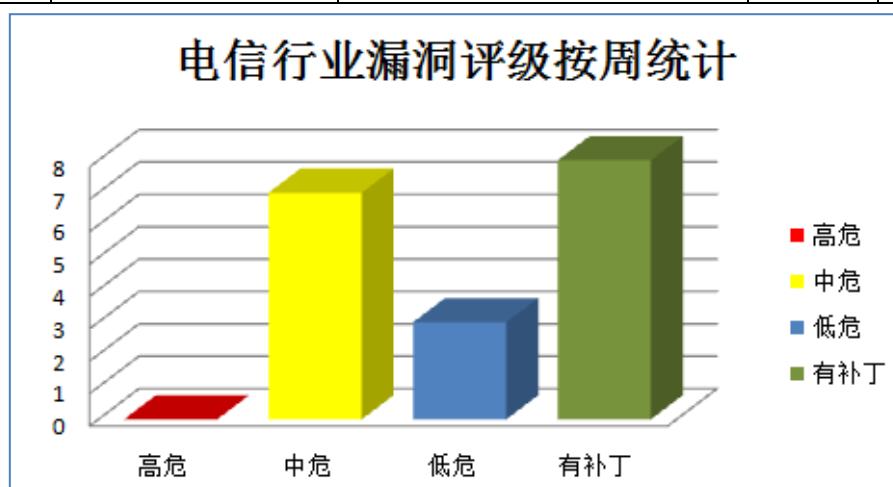


图 1 电信行业漏洞统计

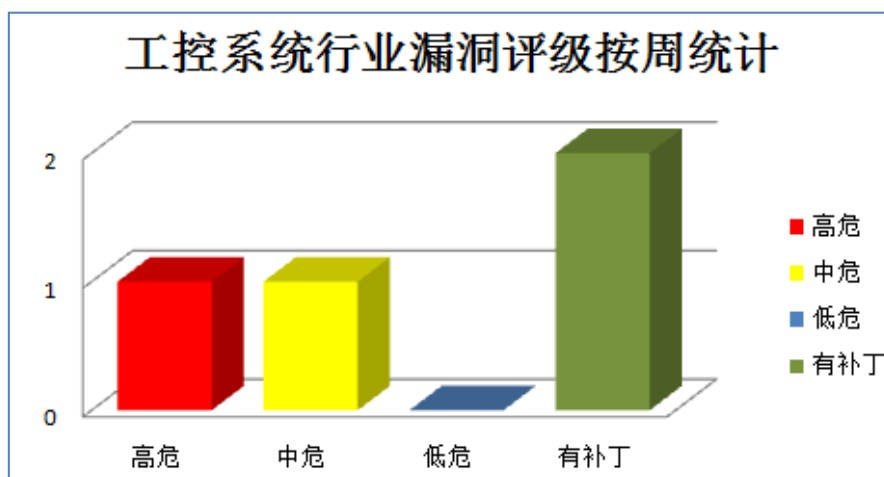


图2 工控系统行业漏洞统计

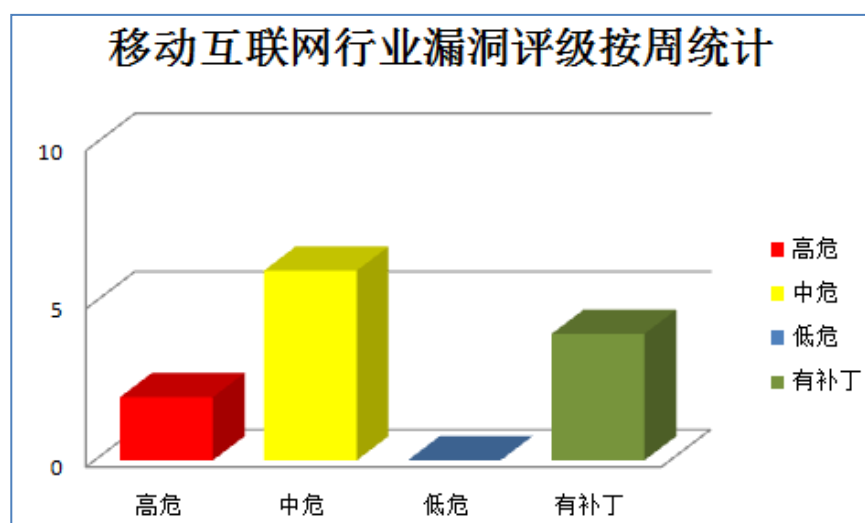


图3 移动互联网行业漏洞

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、Microsoft 产品安全漏洞

Microsoft Word 2003 是一款文件处理程序；Microsoft Internet Explorer 是一款 WEB 浏览器。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可使应用程序崩溃，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft Word 2003 特制.doc 文件处理拒绝服务漏洞、Microsoft Internet Explorer 存在未明远程代码执行漏洞（CNVD-2013-14548）、Microsoft Windows win32k.sys IsHandleEntrySecure 空指针引用本地拒绝服务漏洞。其中，除“Microsoft Windows win32k.sys IsHandleEntrySecure 空指针引用本地拒绝服务漏洞”外，其余漏洞的综合评级均为“高危”。厂商尚未发布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-2013-14590>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14548>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14591>

2、Linux 安全漏洞

Linux 是一款开源的操作系统; Linux Kernel IP Virtual Server 是内核传输层负载平衡器。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, 提升特权, 导致拒绝服务攻击。

CNVD 收录的相关漏洞包括: Linux Kernel 远程拒绝服务漏洞(CNVD-2013-14512)、Linux Kernel IP 虚拟服务器栈缓冲区溢出漏洞、Linux Kernel 本地权限提升漏洞(CNVD-2013-14536)、Linux Kernel '__nfs4_get_acl_uncached()'函数本地缓冲区溢出漏洞、Linux kernel 'ath9k_htc_set_bssid_mask'信息泄露漏洞、Linux Kernel 'kvm_main.c'本地拒绝服务漏洞。其中, “Linux Kernel 远程拒绝服务漏洞(CNVD-2013-14512)、Linux Kernel IP 虚拟服务器栈缓冲区溢出漏洞”的综合评级均为“高危”。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安全事件。

参考链接: <http://www.cnvd.org.cn/flaw/show/CNVD-2013-14512>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14571>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14536>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14563>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14598>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14562>

3、IBM 产品安全漏洞

IBM Cognos 是一款集成商业智能(BI)和计划的解决方案; IBM WebSphere Application Server 是一款商业性质的 WEB 应用服务程序; WebSphere Virtual Enterprise(WVE)是 IBM 实现中间件虚拟化的核心产品。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, 使应用程序崩溃。

CNVD 收录的相关漏洞包括: IBM Cognos Business Intelligence 远程拒绝服务漏洞、IBM Cognos Business Intelligence XML 外部实体信息泄露漏洞、IBM WebSphere Application Server 存在未明跨站脚本漏洞、IBM WebSphere Application Server 管理控制台存在未明反射型跨站脚本漏洞、IBM WebSphere Application Server 迁移角色分配权限提升漏洞、IBM WebSphere Virtual Enterprise 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-2013-14631>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14632>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14550>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14549>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14551>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14516>

4、Apple 产品安全漏洞

Apple iOS 是由苹果公司为移动设备所开发的操作系统，支持的设备包括 iPhone、iPod touch、iPad、Apple TV。本周，该产品被披露存在多个漏洞，攻击者利用漏洞可绕过安全限制，执行未经授权的操作。

CNVD 收录的相关漏洞包括：Apple iOS 本地安全绕过漏洞（CNVD-2013-14510）、Apple iOS Safari Mobile Web Browser 存在多个漏洞。厂商已发布了“Apple iOS 本地安全绕过漏洞（CNVD-2013-14510）”的修补程序。CNVD 提醒相关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-2013-14510>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14511>

5、MyBB Ajax forum stat Plugin 'ajaxfs.php'存在多个 SQL 注入漏洞

MyBB Ajax forum stat Plugin 是一款用于 MyBB 的统计插件。本周，MyBB Ajax forum stat Plugin 被披露存在一个综合评级为“高危”的 SQL 注入漏洞。MyBB Ajax forum stat Plugin 多个脚本未能正确过滤用户提交的输入，远程攻击者利用漏洞可提交特制的 SQL 查询，操作或获取数据库信息。目前，互联网上已经出现了针对该漏洞的攻击代码，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-2013-14611>

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-2013-14595	SAP NetWeaver 远程代码执行漏洞	高	用户可联系厂商获取最新本： http://www.sap.com/index.html
CNVD-2013-14636	Red Hat Network Satellite 安全绕过漏洞	高	请安装厂商已发布的最新版本或补丁： https://access.redhat.com/site/articles/539283
CNVD-2013-14634	vBulletin 存在未明漏洞	高	暂无
CNVD-2013-14639	SPIP 'ecran_securite.php'PHP 代码注入漏洞	高	请联系厂商下载已发布的最新版本或补丁： http://www.spip.net/

CNVD-2013-14610	PineApp Mail-SeCure 本地权限提升漏洞	高	暂无
CNVD-2013-14633	HP Integrated Lights-Out 存在未明跨站脚本漏洞	高	请安装厂商已发布的最新版本或补丁： https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c03996804
CNVD-2013-14617	Kaseya UploadImage 任意文件上传漏洞	高	Kaseya 6.3.2 已经修复该漏洞，建议用户下载更新： http://www.kaseya.co.za/solutions.aspx
CNVD-2013-14573	Intersystems Cache Default 'Minimal Security' 安装远程代码执行漏洞	高	暂无
CNVD-2013-14574	EMC Document Sciences xPression 存在未明 HTML 注入漏洞	高	用户可联系供应商获得补丁信息： http://www.emc.com/index.htm?fromGlobalSiteSelect
CNVD-2013-14582	Mozilla Network Security Services 远程执行任意代码漏洞	高	厂商已经发布了升级补丁以修复这个漏洞，请到厂商的主页下载： https://developer.mozilla.org/zh-CN/docs/NSS/NSS_3.15.3_release_notes

表 3 部分高危漏洞列表

小结：本周，Apple iOS 和 Microsoft、Linux、IBM 多款产品被披露存在多个漏洞，攻击者利用漏洞可绕过权限限制获得敏感信息，导致拒绝服务攻击等。此外，MyBB Ajax forum stat Plugin 插件被披露存在一个高危零日漏洞，建议相关用户应随时关注厂商主页，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 Integrated Lights-Out 4 (iLO4) 产品安全漏洞

HP Integrated Lights-Out 用于对服务器的远程管理。HP 修补了 Integrated Lights-Out 4 (iLO4) 产品存在的跨站脚本和信息泄露两个漏洞，避免攻击者利用漏洞注入任意 Web 脚本和 HTML，获取敏感信息。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安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/41236>
<http://www.cnvd.org.cn/patchInfo/show/41234>

本周要闻速递

1. Nginx 爆发“限制失效”漏洞

最近 Nginx 多个版本曝出“限制失效”的高危漏洞(CVE-2013-4547)，可导致黑客绕过 Nginx 的安全规则，直接访问网站服务器禁止访问的目录文件，造成网站数据泄露，或被黑客植入恶意代码。根据 Nginx 官方公告，存在漏洞的版本为 Nginx 0.8.41 - 1.5.6 版本。这些版本已广泛应用于众多国内网站，由于 Nginx 软件中对请求中的空格结尾处理不当，导致该漏洞可以被利用于绕过 nginx 某些访问控制。

参考链接：http://www.cb.com.cn/info/2013_1122/1023916.html

2. Java 应用数据安全漏洞遭利用

攻击者正积极利用一个已知漏洞破坏 JBoss Java EE 应用服务器的数据安全，这些应用服务器以非安全方式向互联网暴露了 HTTP 调用服务。十月初，安全研究员在多家厂商使用 4.X 和 5.X JBoss 的产品中发现了一个漏洞并将之发布。黑客可以利用该漏洞(CVE-2013-4810)在暴露了 EJBInvokerServlet 或 JMXInvokerServlet 上 JBoss 部署上安装一个任意应用。该研究员利用该漏洞安装了一个名改为 pwn.jsp 的 Web Shell 应用，该应用可通过 HTTP 请求在操作系统上执行 Shell 命令。可以通过 OS 的用户身份许可从而运行 JBoss，而在一些 JBoss 部署案例中，甚至可以拥有较高的权限，如管理员。由 IT 厂商的软件漏洞引发的数据安全问题将成为今后信息安全的主流隐患。同时伴随互联网的普及，危险的传播速度和数量也将不断提高。面对这种情况，对于敏感和机密数据采用更具针对性的加密软件进行防护或是一种不错的选择。

参考链接：<http://it.tom.com/network/215864/575652317304b.shtml>

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

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于

构建跨境网络安全事件的快速响应和协调处置机制。截止 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 国际合作伙伴”关系。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999