

信息安全漏洞周报

2013 年 07 月 01 日-2013 年 07 月 07 日

2013 年第 27 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 137 个，其中高危漏洞 36 个、中危漏洞 84 个、低危漏洞 17 个。上述漏洞中，可利用来实施远程攻击的漏洞有 126 个。本周收录的漏洞中，已有 91 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“Mobile USB Drive HD 输入验证漏洞”、“Top Games Script 'gid' SQL 注入漏洞”等的零日攻击代码，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 5 家成员单位和合作伙伴及个人报送了本周收录的全部 137 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、天融信、安天实验室、绿盟科技等单位报送数量较多。此外，天讯瑞达通信技术有限公司和个人报送者向 CNVD 提交了 11 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	105	0
绿盟科技	40	0
安天实验室	79	0
天融信	94	0
恒安嘉新	12	0
天讯瑞达通信技术有限公司	2	2
个人	9	9
报送总计	341	11

录入总计	137（去重）	11
------	---------	----

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 IBM、Wordpress、TYPO3 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	IBM	19	14%
2	Wordpress	16	12%
3	TYPO3	6	4%
4	LOCKON CO.LTD	5	4%
5	Cisco	4	3%
6	HP	4	3%
7	Symantec	3	2%
8	GNU Project	3	2%
9	Atlassian	2	1%
10	Red Hat	1	1%
11	其它	74	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 137 个漏洞。其中应用程序漏洞 81 个，WEB 应用漏洞 41 个，网络设备漏洞 12 个，安全产品漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	81
WEB 应用漏洞	41
网络设备漏洞	12
操作系统漏洞	0
安全产品漏洞	3
数据库漏洞	0

表 3 漏洞按影响类型统计表

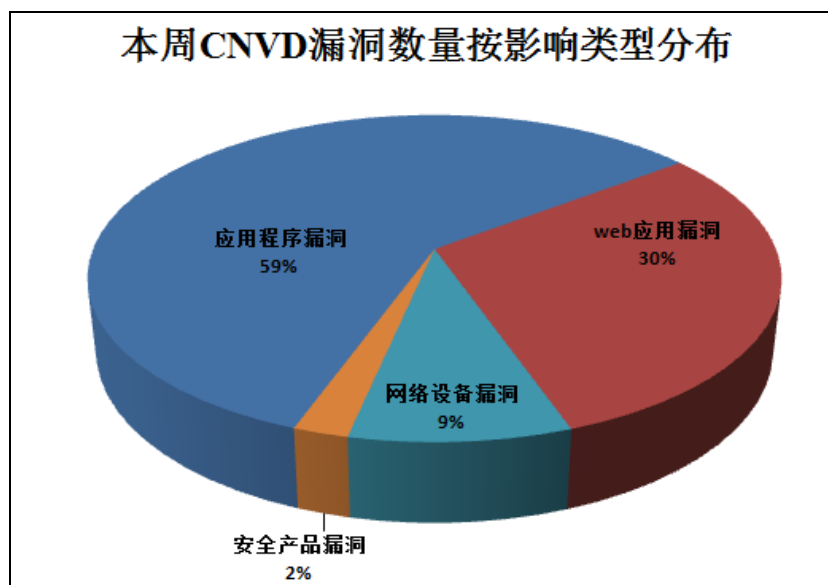


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 12 个网络设备漏洞：多个厂商多个 EAS 设备 SSH 私钥信息泄漏漏洞、Grandstream 多个产品跨站请求伪造漏洞、Grandstream 多个产品 telnet 服务内置账户漏洞、Choice Wireless Green Packet WIXFMR-111 4G WiMac modem 任意命令执行漏洞、多个厂商多个 EAS 设备 WEB 服务器可猜测会话 ID 漏洞、多个厂商多个 EAS 设备 WEB 服务器敏感信息泄漏漏洞、多个厂商多个 EAS 设备默认管理员账户漏洞、多个厂商多个 EAS 设备密码生成不安全漏洞、多个 Cisco Linsys 产品安全绕过漏洞、多个 HP 产品存在未明任意代码执行漏洞（CNVD-2013-27920）、多个 HP 产品存在未明任意代码执行漏洞（CNVD-2013-27921）、ASUS RT-N66U 路由器 AiCloud 安全绕过漏洞。

其中，除“Grandstream 多个产品跨站请求伪造漏洞、Grandstream 多个产品 telnet 服务内置账户漏洞、多个 Cisco Linsys 产品安全绕过漏洞、ASUS RT-N66U 路由器 AiCloud 安全绕过漏洞”外，其余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。

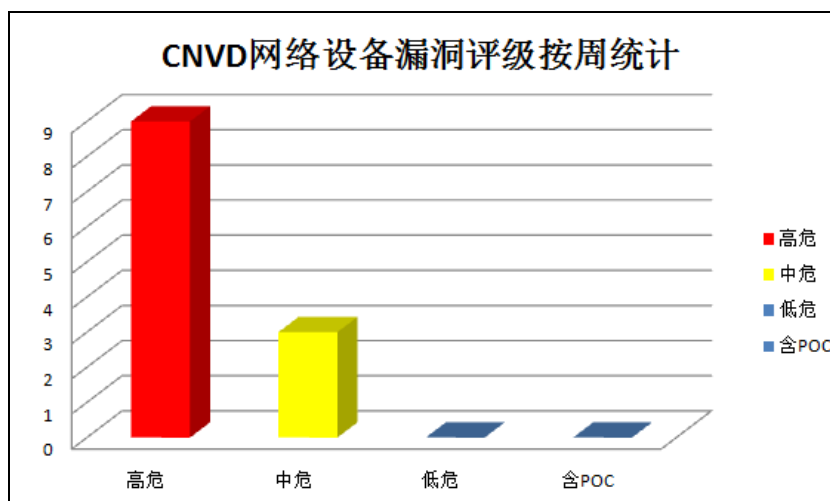


图 2 网络设备漏洞统计

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 IMS Enterprise Suite SOAP Gateway 是一个基于 XML 的解决方案; IBM Sterling B2B Integrator 是实现复杂 B2B 流程安全集成的解决方案。本周，上述产品被披露存在多个安全漏洞，远程攻击者利用漏洞可获得敏感信息，上传任意文件或执行任意代码。

CNVD 收录的相关漏洞包括：IBM IMS Enterprise Suite SOAP Gateway 任意命令执行漏洞、IBM Sterling B2B Integrator 信息泄露漏洞（CNVD-2013-28049、CNVD-2013-28050、CNVD-2013-28054、CNVD-2013-28056、CNVD-2013-28057）、IBM Sterling B2B Integrator 目录遍历漏洞、IBM Sterling B2B Integrator 任意文件上传漏洞等。其中，“IBM IMS Enterprise Suite SOAP Gateway 任意命令执行漏洞”的综合评级为“高危”。厂商已发布上述漏洞的修补程序。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-2013-27917>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28049>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28050>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28051>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28052>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28054>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28056>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28057>

2、Cisco 产品安全漏洞

Cisco Linksys 是思科公司开发的路由器产品；Cisco TelePresence 是一款网真会议解

决方案; Cisco Desktop Collaboration Experience DX650 是思科取代 Cius 的一款目标客户为企业的多功能终端; IronPort 系列产品是加密网关, AsyncOS 是该产品所使用的操作系统; Cisco Content Security Management Appliance 是一款内容安全管理应用设备; Cisco Email Security Appliance 是一个 EMAIL 安全网关。本周, 上述思科产品被披露存在安全漏洞, 攻击者利用漏洞可劫持用户会话, 未授权访问设备或执行任意代码。

CNVD 收录的相关漏洞包括: 多个 Cisco Linsys 产品安全绕过漏洞、Cisco TC Software SIP 实现安全漏洞、Cisco Desktop Collaboration Experience DX650 本地缓冲区溢出漏洞、Cisco 多个产品跨站请求伪造漏洞。厂商已发布了除“多个 Cisco Linsys 产品安全绕过漏洞”外其余漏洞的修补程序。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-2013-27919>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27914>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27913>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27912>

3、EC-CUBE 安全漏洞

EC-CUBE 是一款开源的购物商店建站系统。本周, 该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或执行任意代码。

CNVD 收录的相关漏洞包括: EC-CUBE 任意 PHP 代码执行漏洞、EC-CUBE 任意 PHP 代码执行漏洞、EC-CUBE 跨站脚本漏洞 (CNVD-2013-27753、CNVD-2013-27754)、EC-CUBE 目录遍历漏洞。其中, “EC-CUBE 任意 PHP 代码执行漏洞”的综合评级为“高危”。厂商已发布上述漏洞的修补程序。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-2013-27752>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27751>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27753>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27754>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27755>

4、WordPress 插件安全漏洞

WordPress 是一种使用 PHP 语言开发的博客平台。本周, WordPress 多个插件被披露存在多个漏洞。远程攻击者利用漏洞可劫持用户会话, 执行 SQL 查询或操纵数据库系统, 发起钓鱼攻击。

CNVD 收录的相关漏洞包括: WordPress 插件 WP Private Messages 'msgid' SQL 注入漏洞、WordPress 插件 WP Feed 'nid'参数 SQL 注入漏洞、WordPress Xorbin Digital Flash Clock 'widgetUrl'参数跨站脚本漏洞、WordPress 插件 Category Grid View Gallery 'ID'参数跨站脚本漏洞、WordPress 'post.php'输入验证漏洞、WordPress 'SWFUpload' Library 跨站

脚本漏洞、WordPress 服务端请求伪造漏洞、WordPress 内容欺骗漏洞等。其中，“WordPress 插件 WP Private Messages 'msgid' SQL 注入漏洞、WordPress 插件 WP Feed 'nid'参数 SQL 注入漏洞”的综合评级均为“高危”。厂商已发布“WordPress 'post.php'输入验证漏洞、WordPress 'SWFUpload' Library 跨站脚本漏洞、WordPress 服务端请求伪造漏洞、WordPress 内容欺骗漏洞”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-2013-27889>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27939>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27890>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27930>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27931>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27932>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27933>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-27938>

5、Top Games Script 'gid' SQL 注入漏洞

Top Games Script 是一款基于 WEB 的应用。本周，该产品被披露存在一个综合评级为“高危”的 SQL 注入漏洞。Top Games Script 'play.php'未能正确过滤用户提交给"gid"参数的数据，远程攻击者利用漏洞可提交恶意 SQL 查询，获取数据库信息或控制应用系统。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-2013-27882>

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-2013-28029	Choice Wireless Green Packet 4G WiMax Modem 信息泄露漏洞	高	暂无
CNVD-2013-27921	多个 HP 产品存在未明任意代码执行漏洞（CNVD-2013-27921）	高	用户可参考如下厂商提供的安全公告获得补丁信息： http://h20565.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?docId=emr_na-c03808969-1
CNVD-2013-27965	TYPO3 RSS feed from records 扩展 SQL 注入漏洞	高	暂无
CNVD-2013-27880	SaltStack Salt 存在多个漏洞	高	Salt 0.15.1 已经修复此漏洞，建议用户下载更新：

			http://www.saltstack.com
CNVD-2013-27962	PCMan FTP Server 'USER'命令缓冲区溢出漏洞	高	暂无
CNVD-2013-27874	GNU ZRTP 存在多个远程栈缓冲区溢出漏洞	高	GNU ZRTP 3.2.0 已经修复此漏洞，建议用户下载更新： https://github.com/wernerd/ZRTPCPP 或可参考如下厂商提供的安全公告获得补丁信息： https://github.com/wernerd/ZRTPCPP/commit/c8617100f359b217a974938c5539a1dd8a120b0e
CNVD-2013-27941	Joomla! com_football 组件'teamID'参数 SQL 注入漏洞	高	暂无
CNVD-2013-27761	JS-YAML Node.js 模块任意代码执行漏洞	高	JS-YAML Node.js Module 2.1.0 已经修复此漏洞，建议用户下载更新： https://npmjs.org/package/js-yaml
CNVD-2013-27915	FreeSWITCH 'switch_regex.c'缓冲区溢出漏洞	高	暂无
CNVD-2013-27866	Atlassian Crowd 存在未明后门漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，IBM 多款产品和 EC-CUBE 购物商店系统以及 WordPress 的多个插件被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息，执行任意代码或钓鱼攻击。Cisco 的多款设备被披露存在漏洞，攻击者利用漏洞可劫持用户会话，未经授权访问设备，相关企业用户应注意加强防范上述漏洞威胁。此外，Top Games Script 被披露存在高危零日漏洞，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、Red Hat 发布升级程序，修补 Enterprise Virtualization Manager 安全漏洞

Red Hat Enterprise Virtualization Manager 是一款虚拟化解决方案应用。本周，Red Hat 发布升级程序，修补了 Enterprise Virtualization Manager 存在的拒绝服务漏洞。攻击者可以通过克隆快照的虚拟机导致拒绝服务。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/34971>



本周要闻速递

1. 安卓曝新漏洞

近日，美国移动安全公司 Bluebox 宣布发现了安卓系统的一个特大漏洞。该漏洞可令黑客读取用户数据、获取密码，并控制手机的任何功能，包括发送短信、拨打电话或打开摄像头等。黑客可以通过这个漏洞，在不改变应用密钥签名的情况下篡改安装包代码，这对于用户来说无疑非常危险。Bluebox 公司表示，该木马可以读取设备上任意手机应用的数据，获取保存在手机上的所有账号和密码，接管并控制手机的正常功能。据介绍，今年 2 月时这个 bug 已经被披露给了 Google 公司，但解决办法目前尚未出台。

参考链接：<http://article.pchome.net/content-1632214.html>

2. 微软 IE8 浏览器再曝安全漏洞

据报道，微软公司的 IE 浏览器近日又曝出新的“0Day”漏洞，该漏洞影响 IE8 浏览器，无论是个人电脑还是企业网络用户，均有可能因此遭到黑客攻击。据安全专家分析，虽然目前已知的攻击代码只针对 Windows XP 系统下的 IE8 浏览器，但该漏洞也可以用来攻击 Windows 7 系统，预计短期内针对 Windows 7 的攻击代码就会被黑客开发并利用。利用该漏洞，黑客可在用户访问恶意网页时执行任意代码，并借助这些代码下载木马或病毒程序，进而对用户发起攻击。

参考链接：<http://it.msn.com.cn/network/421068/591734126909b.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