

信息安全漏洞周报

2013 年 10 月 28 日-2013 年 11 月 03 日

2013 年第 44 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 116 个，其中高危漏洞 36 个、中危漏洞 70 个、低危漏洞 10 个。上述漏洞中，可利用来实施远程攻击的漏洞有 102 个。本周收录的漏洞中，已有 75 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“WordPress AREA53 Theme 'php.php'任意文件上传漏洞”、“PHPCMS Guestbook 存在多个 HTML 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 4 家成员单位和一家公司及个人报送了本周收录的全部 116 个漏洞。报送情况如表 1 所示。其中，安天实验室、绿盟等单位报送数量较多。此外，深圳市腾讯计算机系统有限公司和个人报送者向 CNVD 提交了 4 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
安天实验室	163	0
绿盟科技	111	0
启明星辰	56	0
恒安嘉新	56	0
深圳市腾讯计算机系统有限公司	1	1
个人	3	3
报送总计	389	4
录入总计	116（去重）	4

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 cPanel、wordpress、Mozilla 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	cPanel	12	10%
2	wordpress	11	9%
3	Mozilla	6	5%
4	Cisco	6	5%
5	IBM	4	3%
6	Apache	3	3%
7	OBM-Media e.K. Internetsolutions	3	3%
8	Poppler	3	3%
9	Linux	1	1%
10	其它	67	58%

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 116 个漏洞。其中应用程序漏洞 52 个，WEB 应用漏洞 45 个，操作系统漏洞 5 个，网络设备漏洞 12 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	52
WEB 应用漏洞	45
网络设备漏洞	12
操作系统漏洞	5
安全产品漏洞	2
数据库漏洞	0

表 3 漏洞按影响类型统计表

本周CNVD漏洞数量按影响类型分布

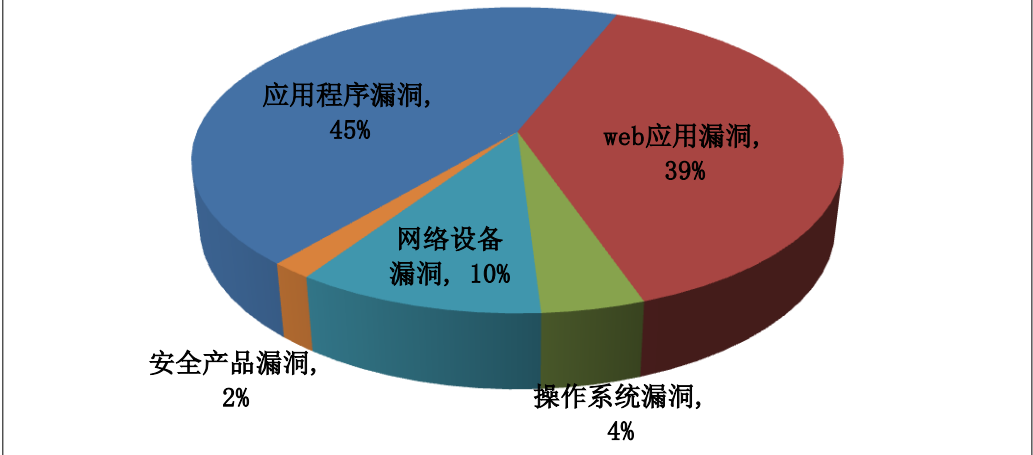


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 11 个电信行业漏洞和 1 个工控系统行业漏洞(如下列表所示)。其中，“NETGEAR WNDR3700 'sprintf()'函数特制 Host 字符串缓冲区溢出漏洞、Netgear WNDR3700 Router 'cmd_ping6()'远程命令注入漏洞、Cisco IOS XR Software 分片报文处理拒绝服务漏洞、VICIDIAL 'manager_send.php' SQL 注入漏洞、VICIDIAL 'manager_send.php'命令注入漏洞”的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。本周，CNVD 未收录移动互联网行业漏洞。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-14195	ASUS RT-N13U 路由器未授权 ROOT 访问漏洞	中	否
电信	CNVD-2013-14198	ADB Discus DRG A125G 'wansinglecfg.cmd'密码泄露漏洞	中	否
电信	CNVD-2013-14178	Cisco Unified Communications Manager 拒绝服务漏洞（CNVD-2013-14178）	中	是
电信	CNVD-2013-14125	NETGEAR WNDR3700 'sprintf()'函数特制 Host 字符串缓冲区溢出漏洞	高	否
电信	CNVD-2013-14126	Netgear WNDR3700 Router 'cmd_ping6()'远程命令注入漏洞	高	否
电信	CNVD-2013-14155	Netgear WNDR3700 Router 存	中	否

		在多个验证绕过漏洞		
电信	CNVD-2013-14149	Cisco IOS XR Software 分片报文处理拒绝服务漏洞	高	是
电信	CNVD-2013-14094	Cisco Identity Services Engine Guest 用户帐户耗尽拒绝服务漏洞	中	是
电信	CNVD-2013-14084	Cisco Catalyst 3750 Series Switches 默认证书凭证绕过漏洞	中	是
电信	CNVD-2013-14088	VICIDIAL 'manager_send.php' SQL 注入漏洞	高	否
电信	CNVD-2013-14089	VICIDIAL 'manager_send.php' 命令注入漏洞	高	否
工控系统	CNVD-2013-14172	Cogent DataHub 拒绝服务漏洞	中	是

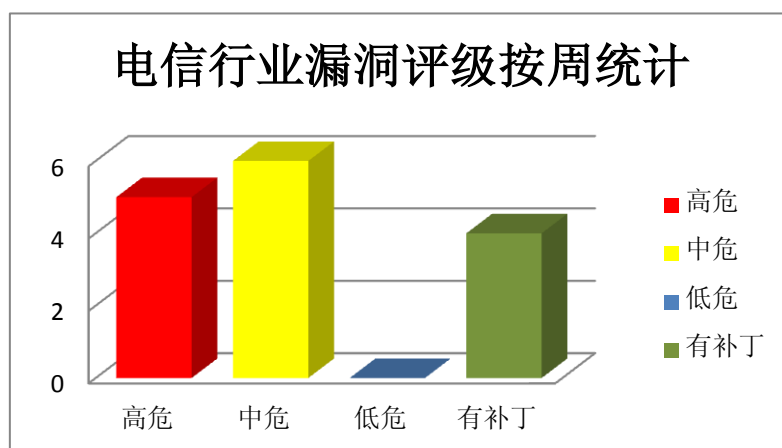


图 1 电信行业漏洞统计

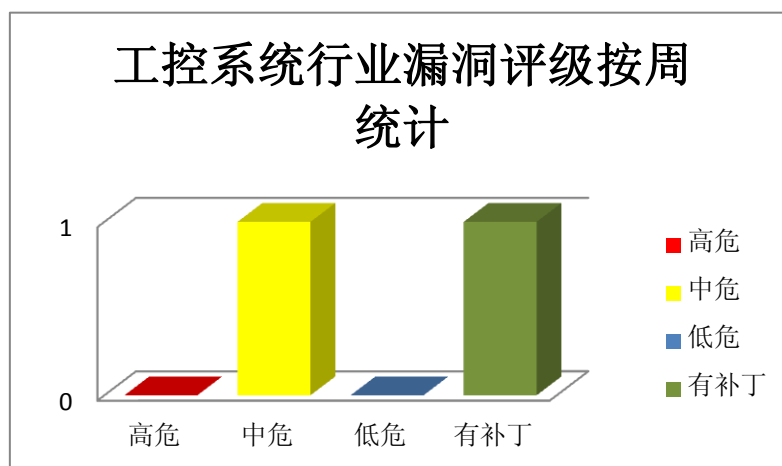


图 2 工控系统行业漏洞统计

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。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，导致拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox PDF.js 子帧注入任意系统文件泄漏漏洞、Mozilla 多个产品 nsDocLoader::doStopDocumentLoad()函数内存错误引用漏洞、Mozilla Firefox 存在未明内存破坏漏洞、Mozilla 多个产品超大页图像对象收集处理竞争条件漏洞、Mozilla 多个产品 JavaScript 引擎内存分配存在多个缓冲区溢出漏洞、Mozilla 多个产品 select 元素处理 URL 栏伪造漏洞。其中，“Mozilla Firefox PDF.js 子帧注入任意系统文件泄漏漏洞、Mozilla 多个产品 nsDocLoader::doStopDocumentLoad()函数内存错误引用漏洞、Mozilla Firefox 存在未明内存破坏漏洞”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-2013-14179>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14180>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14184>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14181>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14182>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14183>

2、Netgear 产品安全漏洞

Netgear WNDR3700 是一款路由器设备；NetGear RAIDiator 是基于 Linux 和 debian-sparc 平台的直接挂网存储设备。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，执行未授权的访问，或执行任意命令。

CNVD 收录的相关漏洞包括：NETGEAR WNDR3700 'sprintf()'函数特制 Host 字符串缓冲区溢出漏洞、Netgear WNDR3700 Router 'cmd_ping6()'远程命令注入漏洞、NetGear RAIDiator 命令注入漏洞、Netgear WNDR3700 Router 存在多个验证绕过漏洞、NetGear RAIDiator 跨站请求伪造漏洞。其中，“NETGEAR WNDR3700 'sprintf()'函数特制 Host 字符串缓冲区溢出漏洞、Netgear WNDR3700 Router 'cmd_ping6()'远程命令注入漏洞、NetGear RAIDiator 命令注入漏洞”的综合评级均为“高危”。厂商已经发布了“NetGear RAIDiator 命令注入漏洞、NetGear RAIDiator 跨站请求伪造漏洞”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-2013-14125>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14126>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14090>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14155>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14091>

3、Cisco 产品安全漏洞

Cisco IOS XR 是基于微内核分配操作系统架构；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 Unified Communications Manager 是企业级 IP 电话呼叫处理系统；Cisco Identity Services Engine 身份服务引擎一款用于 Cisco TrustSec 解决方案的中央策略引擎；Cisco Catalyst 3750 系列交换机是一款创新交换机。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，使设备重启，导致拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IOS XR Software 分片报文处理拒绝服务漏洞、Cisco Adaptive Security Appliance (ASA) 远程拒绝服务漏洞、Cisco Adaptive Security Appliance (ASA) 远程拒绝服务漏洞、Cisco Identity Services Engine 远程验证绕过漏洞、Cisco Identity Services Engine Guest 用户帐户耗尽拒绝服务漏洞、Cisco Catalyst 3750 Series Switches 默认证书凭证绕过漏洞。其中，“Cisco IOS XR Software 分片报文处理拒绝服务漏洞”的综合评级为“高危”。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-2013-14149>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14177>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14178>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14150>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14094>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14084>

4、cPanel 组件安全漏洞

cPanel 是一款基于多种语言的空间管理面板，可通过域名来管理整个站点。本周，该产品被披露存在多个漏洞，攻击者利用漏洞可提升特权，使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：cPanel 多个组件特制 POST 请求任意文件操作漏洞、cPanel WHM Apache mod_userdir Tweak 接口远程命令执行漏洞、cPanel Webmail/Demo 账户权限绕过任意文件删除漏洞、cPanel WHM 配置客户联系人接口 jailshell 限制绕过远程权限提升漏洞、cPanel WHM logaholic_lang cookie 处理存在未明远程命令执行漏洞、cPanel /usr/local/cpanel/base/3rdparty/Logaholic 目录权限特权提升漏洞、cPanel WHM Mailman Pickle 文件处理本地权限提升漏洞、cPanel 特制 SSL 证书上传远程拒绝服务漏洞等。其中，除“cPanel /usr/local/cpanel/base/3rdparty/Logaholic 目录权限特权提升漏洞、cPanel WHM Mailman Pickle 文件处理本地权限提升漏洞、cPanel 特制 SSL 证书上传远

程拒绝服务漏洞”外，其余漏洞的综合评级均为“高危”。厂商已发布了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-2013-14144>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14141>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14139>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14138>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14137>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14134>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14136>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14142>

5、WordPress AREA53 Theme 'php.php'任意文件上传漏洞

WordPress 是一款基于 PHP 的博客平台，用户可以在支持 PHP 和 MySQL 数据库的服务器上架设自己的网志。本周，WordPress AREA53 Theme 被披露存在一个综合评级为“高危”的文件上传漏洞。由于程序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文件，并以 WEB 权限执行。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-2013-14100>

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-2013-14165	Juniper Networks Junos Proxy ARP 拒绝服务漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://kb.juniper.net/InfoCenter https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10595
CNVD-2013-14169	GTX CMS 存在多个 SQL 注入漏洞	高	暂无
CNVD-2013-14122	Poppler 'utils/pdfseparate.cc' 文件栈缓冲区溢出漏洞	高	poppler 0.24.2 已经修复该漏洞，建议用户下载更新： http://poppler.freedesktop.org/
CNVD-2013-14113	Onpub SQL 注入漏洞	高	暂无
CNVD-2013-14087	RoundCube Webmail '_session'处理数据操纵漏洞	高	RoundCube Webmail 0.8.7 或 0.9.5 已修复此漏洞，建议用户下载使用： http://roundcube.net/

CNVD-2013-14118	VideoCharge Studio '.vsc'文件处理缓冲区溢出漏洞	高	暂无
CNVD-2013-14093	SMF 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.simplemachines.org/
CNVD-2013-14119	Symantec Workspace Streaming SWS Streamlet 引擎服务 Marshalled 对象远程命令执行漏洞	高	暂无
CNVD-2013-14153	RSA Authentication Agent For Web For IIS 安全绕过漏洞	高	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： https://knowledge.rsasecurity.com
CNVD-2013-14127	Nagios Looking Glass 本地文件包含漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，cPanel 和 Mozilla、Cisco、Netgear cPanel 的多款产品被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息，导致拒绝服务攻击或执行任意代码。此外，WordPress AREA53 Theme 程序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、Linux 修补内核本地内存破坏漏洞

Linux Kernel 是一款开源的操作系统，Linux 内核内置的启用的 UDP UFO 功能的以太驱动程序(virtio-net)在设置 UDP_CORK 套接字选项时存在内存破坏漏洞，攻击者可发送大量消息(其中不是所有的消息都大于相关系统的最大传输单元(MTU))可触发该漏洞。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/40566>

本周要闻速递

1. GSM 通信显安全漏洞

据新华社电，GSM 通信存在安全风险漏洞，一旦被黑客破解，GSM 手机用户的重要信息将面临威胁。据了解，GSM 是全球应用最广泛的移动电话标准，就是大家普遍熟知的 G 网手机 SIM 卡。一旦手机短信内容被黑客截获，手机号码所绑定的网上支付、

电子邮箱、聊天账号等重要信息将全部面临被盗风险，手机使用者在支付和验证身份时，将面临严重安全威胁。因此，GSM 手机用户收到各种短信验证内容时应提高警惕，一旦发现不是由自己发起的网上支付或“找回密码”短信，应立即联系银行和支付平台客服求助。此外，网民应注意对个人信息严格保密，以免身份证号等重要信息泄露。

参考链接：<http://tech.hexun.com/2013-11-04/159329273.html>

2. 埃及专家发现 facebook 存安全漏洞

中国网 11 月 1 日讯，据卡塔尔半岛电视台网站 10 月 30 日报道，埃及一名安全专家发现美国 facebook 公司应用程序中两个被称之为“重大危险”的漏洞，无论是在 facebook 的基本社交软件，或是即时信息软件，亦或是 facebook 网页管理器中，都存在该漏洞，特别是应用安卓系统时候。在安卓系统中，通过两个漏洞可以从 facebook 的账户进入到该设备中安装的其他应用程序中，窃取到用户信息。在安卓系统中，通过两个漏洞可以从 facebook 的账户进入到该设备中安装的其他应用程序中，窃取到用户信息。这两个漏洞能窃取安卓系统用户日志中的登录信息，被称为 logcat，从而使其他的应用程序能够获得日志备份，储存在服务器中，从而获取用户信息，控制其 facebook 账户。得知消息以后，facebook 安全团队立即修复了漏洞，同时也表示将给该埃及专家提供 6000 美元，作为发现这两个漏洞的奖金。据消息称，上周一 facebook 已经更新了基本社交程序和网页管理器程序，而昨天，也推出了即时信息软件的更新，据称，这些应用程序的网页正在进行漏洞修复。

参考链接：http://www.china.com.cn/news/world/2013-11/01/content_30466870.htm

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