

信息安全漏洞周报

2012 年 9 月 3 日-2012 年 9 月 10 日

2012 年第 36 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 141 个，其中高危漏洞 28 个、中危漏洞 96 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 128 个。本周收录的漏洞中，已有 104 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“Mcrypt 栈缓冲区溢出漏洞”、“Wireshark 远程界面缓冲区溢出漏洞”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 7 家成员单位和多个合作伙伴报送了本周收录的全部 141 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技、天融信、安天实验室等单位报送数量较多。此外，来自 High-Tech Bridge Security Research Lab 以及个人漏洞研究者向 CNVD 提交了 5 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	113	0
启明星辰	135	0
安天实验室	60	0
恒安嘉新	2	0
天融信	38	0
安氏领信	9	0
知道创宇	1	0
High-Tech Bridge Security Research Lab	3	3

个人报送者	2	2
报送总计	363	5
录入总计	141（去重）	5

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 HP、Symantec、IBM、Linux 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	12	8%
2	HP	3	2%
3	ownCloud	11	8%
4	TYPO3	9	6%
5	Bugzilla	2	1%
6	WordPress	3	2%
7	Linux	3	2%
8	Drupal	10	7%
9	Adobe	1	1%
10	Apache	3	2%
11	其它	84	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 141 个漏洞。其中操作系统漏洞 3 个，应用程序漏洞 82 个，WEB 应用漏洞 53 个，网络设备漏洞 2 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	3
应用程序漏洞	82
WEB 应用漏洞	53
网络设备漏洞	2
数据库漏洞	0
安全产品漏洞	1

表 3 漏洞按影响类型统计表

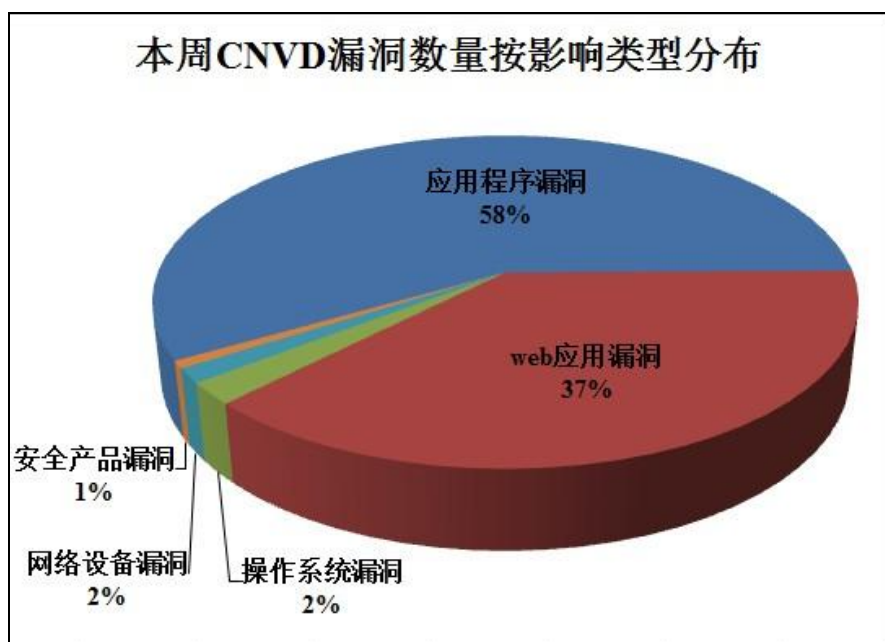


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 2 个网络设备漏洞：“Arbiter Systems Power Sentinel 拒绝服务漏洞（CNVD-2012-14283）、ZTE ZXDSL 跨站请求伪造漏洞”。其中，“Arbiter Systems Power Sentinel 拒绝服务漏洞（CNVD-2012-14283）”的综合评级均为“高危”。目前，互联网上已经出现了针对“ZTE ZXDSL 跨站请求伪造漏洞”的攻击代码。

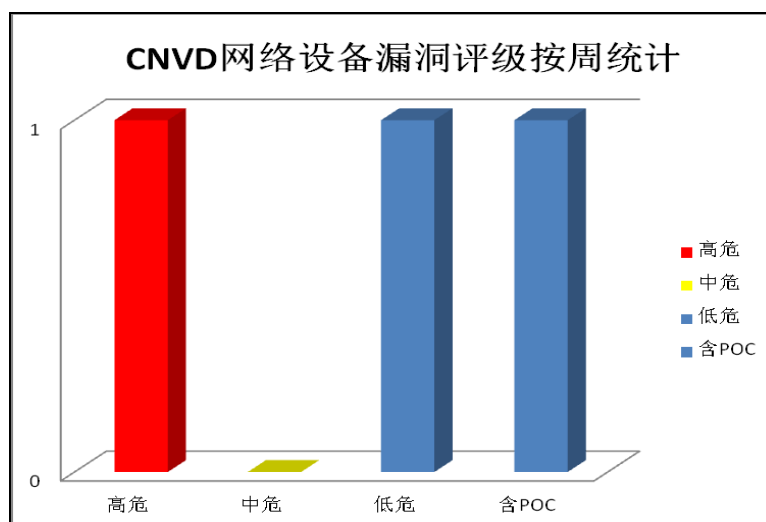


图 2 网络设备漏洞统计

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、Google 产品安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。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劫持用户会话，使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome line-breaking 越界读漏洞、Google Chrome SPDY 拒绝服务漏洞、Google Chrome run-ins 类型转换漏洞、Google Chrome workers 和 XHR 竞争条件漏洞、Google Chrome URL 加载漏洞、Google Chrome 内存管理漏洞、Google Chrome SSL interstitial 跨站脚本漏洞、Google Chrome XSL Transform 类型转换漏洞。厂商已经修复了上述漏洞，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/sites/main/preview/ldgg_preview.htm?tid=55500
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55515
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55501
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55519
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55522
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55524
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55534
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55529

2、ownCloud 安全漏洞

ownCloud 是一款开源的私有云服务软件。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劫持用户会话，以 WEB 权限执行恶意上传的 PHP 代码，控制应用系统。

CNVD 收录的相关漏洞包括：ownCloud 存在多个跨站脚本漏洞（CNVD-2012-14304）、ownCloud 配置文件编辑漏洞、ownCloud 验证绕过漏洞、ownCloud 不完整黑名单任意代码执行漏洞、ownCloud 用户枚举漏洞、ownCloud 请求伪造漏洞、ownCloud 跨站请求伪造漏洞（CNVD-2012-14308）、ownCloud 跨站脚本漏洞（CNVD-2012-14307）等。其中，“ownCloud 不完整黑名单任意代码执行漏洞”的综合评级为“高危”。目前，厂商已经修复了上述漏洞。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/sites/main/preview/ldgg_preview.htm?tid=56302
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56300
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56195
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56198
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56197
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56196

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56355

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56335

3、TYPO3 安全漏洞

TYPO3 是一个开源的内容管理系统。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劫持用户会话，并执行任意代码。

CNVD 收录的相关漏洞包括：TYPO3 安装工具跨站脚本漏洞、TYPO3 后端跨站脚本漏洞、TYPO3 不完整黑名单跨站脚本漏洞、TYPO3 configuration 模块加密密钥泄露漏洞、TYPO3 Extbase Framework 任意代码执行漏洞、TYPO3 数据库名信息泄露漏洞、TYPO3 t3lib_div::RemoveXSS API 方法安全绕过漏洞、TYPO3 后端组件跨站脚本漏洞等。目前，厂商已经修复了上述漏洞。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/sites/main/preview/ldgg_preview.htm?tid=56199

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56201

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56215

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56200

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56177

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56175

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56155

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56176

4、Oracle 产品安全漏洞

Java Runtime Environment 是一款为 JAVA 应用程序提供可靠的运行环境的解决方案。本周，该产品被披露存在多个漏洞，攻击者利用漏洞，构建恶意 WEB 页，诱使用户解析，执行任意代码。

CNVD 收录的相关漏洞包括：Oracle Java Runtime Environment 远程代码执行漏洞（CNVD-2012-13961）、Oracle Java Runtime Environment 远程代码执行漏洞（CNVD-2012-13964）、Oracle Java Runtime Environment 存在未明远程代码执行漏洞。上述漏洞的综合评级均为“高危”。目前，厂商已经修复“Oracle Java Runtime Environment 远程代码执行漏洞（CNVD-2012-13961）”和“Oracle Java Runtime Environment 远程代码执行漏洞（CNVD-2012-13964）”。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/sites/main/preview/ldgg_preview.htm?tid=55575

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55578

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55678

5、Wireshark 远程界面缓冲区溢出漏洞

Wireshark（曾用名 Ethereal）是一款网络分组分析软件。本周，Wireshark 被披露存

在一个综合评级为“高危”的缓冲区溢出漏洞。远程攻击者可以利用漏洞执行任意代码。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/sites/main/preview/ldgg_preview.htm?tid=55699

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/publish/main/52/index.html>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2012-14296	Xen 'GNTTABOP_swap_grant_ref' 拒绝服务漏洞	高	用户可参考供应商提供的安全公告获得补丁信息： http://lists.xen.org/archives/html/xen-announce/2012-09/msg00004.html
CNVD-2012-14283	Arbiter Systems Power Sentinel 拒绝服务漏洞（CNVD-2012-14283）	高	厂商已经提供升级程序修复此漏洞： http://www.arbiter.comhttp://www.arbiter.com/files/software/1133/1133a_firmware_v421.zip
CNVD-2012-14261	Siche Search 'ssearch.php' SQL 注入漏洞	高	暂无
CNVD-2012-14266	Group-Office 'sort' SQL 注入漏洞	高	Group-Office 4.0.90 已经修复此漏洞，建议用户下载使用： http://www.group-office.com/
CNVD-2012-14258	phpcms v9 SQL 注入漏洞	高	暂无
CNVD-2012-14253	Adobe Photoshop 远程缓冲区溢出漏洞（CNVD-2012-14253）	高	Adobe Photoshop CS6 (13.0.1)已经修复此漏洞，建议用户下载使用： http://blogs.adobe.com/photoshopdotcom/2012/08/photoshop-cs6-13-0-1-update-now-available.html
CNVD-2012-14166	Joomla! iCagenda 组件'id' SQL 注入漏洞	高	暂无
CNVD-2012-14160	CyberLink PowerProducer 多个 DLL 任意代码执行漏洞	高	暂无
CNVD-2012-14164	Internet Download Manager '.ef2'文件缓冲区溢出漏洞	高	暂无
CNVD-2012-14171	Admidio SQL 注入漏洞	高	Admidio 2.3.6 版本已修复此漏洞，建议用户下载使用： http://www.admidio.org/

CNVD-2012-13924	EMC NetWorker 'nsrd' RPC 服务格式串漏洞	高	EMC NetWorker 7.6.4.1 及之后版本和 EMC NetWorker 8.0.0.1 及之后版本已经修复此漏洞，建议用户下载使用： https://support.emc.com/products/1095_NetWorker
-----------------	----------------------------------	---	--

表 3 部分高危漏洞列表

小结：本周，Google Chrome、ownCloud、TYPO3、Java Runtime Environment 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劫持用户会话，使应用程序崩溃或执行任意代码，控制应用系统。此外，Wireshark 分析软件也被披露存在高危零日漏洞，请相关用户加强防范。另外值得重点关注的是 phpcms v9 存在的一个 SQL 注入漏洞，根据 CNVD 处置工作经验，该软件在基础电信运营企业及相关互联网业务经营者的网站建设中应用较多。

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、Adobe 发布升级程序，修补 Photoshop 漏洞

Adobe Photoshop 是一款流行的图像处理软件。本周，Adobe 发布升级程序，修补了 Photoshop 存在的漏洞。攻击者利用漏洞可构建恶意文件，诱使应用程序解析，执行任意代码。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/sites/main/preview/bdgg_preview.htm?tid=21336

本周要闻速递

1. 微软发布九月份安全补丁

9月7日消息，微软发布九月份安全补丁提前通知，将发布2个补丁修复3个漏洞，包含2个“重要”级别的安全公告将修复3个漏洞，涉及开发者工具及服务器软件。无需用户重启计算机，请打开 Windows 自动更新，及时安装补丁。

参考链接：<http://www.ithome.com/html/soft/25023.htm>

2. 指纹识别软件 UPEK 有大漏洞

据报道，近日有安全研究机构宣称，至少在14家厂商的PC和平板类产品上预装的指纹识别软件存在严重缺陷，能让黑客(在接触到PC的情况下)轻易破解并登录PC。存在这一缺陷的软件是 UPEK Protector Suite，该软件允许用户以自己的指纹作为登录系统密码，比传统登录密码更便捷也更安全。据悉，当这款软件激活后会把登录帐户密码

写到注册表，然后用密钥加密。而这个密钥的强度很一般，一旦被人获取，用不了几秒钟就可以解密。

参考链接：<http://tech.sina.com.cn/s/2012-09-06/08227589120.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的全称是国家计算机网络应急技术处理协调中心（英文简称是 CNCERT 或 CNCERT/CC）成立于 1999 年 9 月，是工业和信息化部领导下的国家级网络安全应急机构，致力于建设国家级的网络安全监测中心、预警中心和应急中心，以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，支持基础信息网络的安全防护和安全运行，支援重要信息系统的网络安全监测、预警和处置；国家互联网应急中心在我国大陆 31 个省、自治区、直辖市设有分中心。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999