

信息安全漏洞周报

2012 年 8 月 13 日-2012 年 8 月 19 日

2012 年第 33 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 118 个，其中高危漏洞 54 个、中危漏洞 56 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 108 个。本周收录的漏洞中，已有 85 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“Spytech NetVizor 远程缓冲区溢出漏洞”、“VLC Media Player '.3gp'文件除零拒绝服务漏洞”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及个人报送了本周收录的全部 118 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、安天实验室等单位报送数量较多。此外，天融信以及个人报送者向 CNVD 提交了 2 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	93	0
绿盟科技	56	0
安天实验室	35	0
恒安嘉新	29	0
天融信	20	1
安氏领信	10	0
东软	3	0
个人报送者	1	1
报送总计	247	2

录入总计	118（去重）	2
------	---------	---

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、ownCloud、HP 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	Adobe	25	21%
2	Microsoft	13	11%
3	ownCloud	7	6%
4	HP	5	4%
5	Joomla!	5	4%
6	ProQuiz	4	3%
7	IBM	3	3%
8	Cisco	2	2%
9	GNU	2	2%
10	Samsung	2	2%
11	其它	50	42%

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 118 个漏洞。其中操作系统漏洞 8 个，应用程序漏洞 94 个，WEB 应用漏洞 14 个，网络设备漏洞 2 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	8
应用程序漏洞	94
WEB 应用漏洞	14
网络设备漏洞	2
数据库漏洞	0
安全产品漏洞	0

表 3 漏洞按影响类型统计表

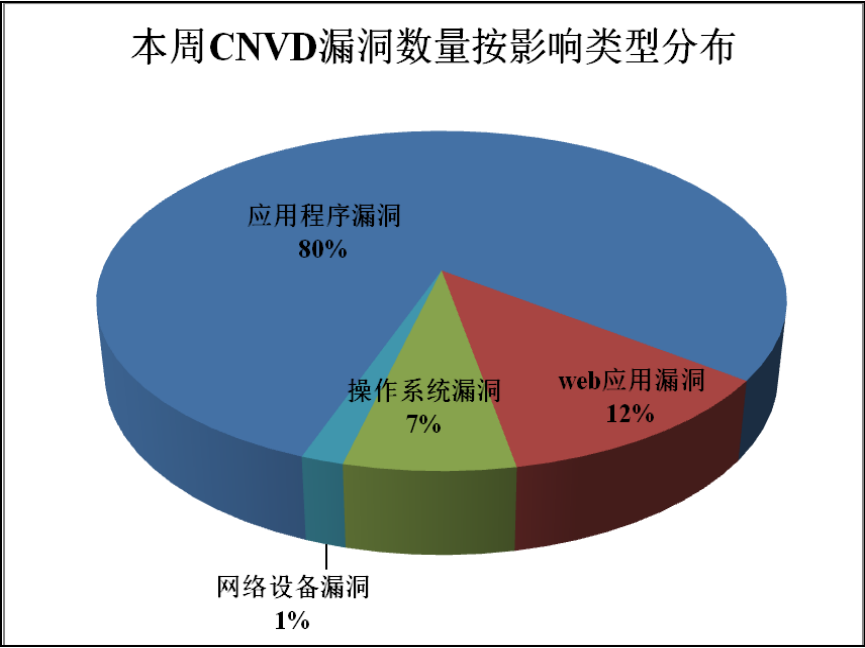


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 2 个网络设备漏洞：“Samsung 和 HTC 设备信息泄露漏洞”和“Samsung Galaxy S2 Epic 4G Touch 不安全临时文件创建漏洞”。

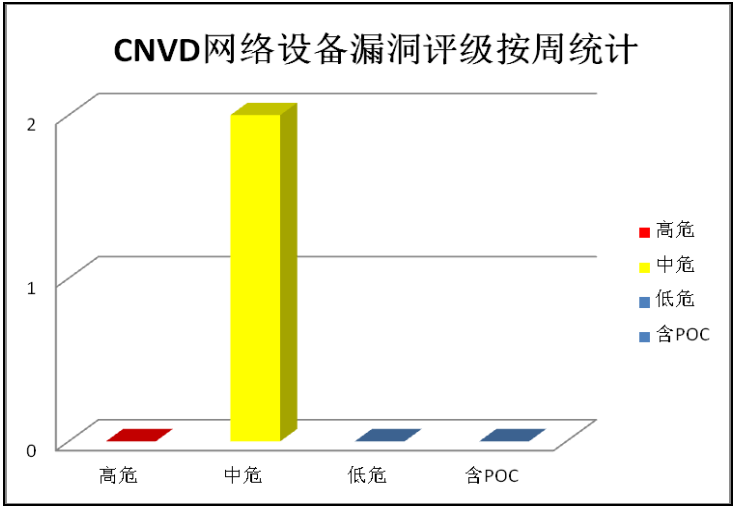


图 2 网络设备漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Internet Explorer 是一款 WEB 浏览器；Microsoft Office 是一款微软开发的

办公软件套件；Microsoft Visio 是一款流程图绘制软件；Microsoft Windows 是一款流行的操作系统。本周，上述 Microsoft 产品被披露存在多个安全漏洞，攻击者利用漏洞可触发整数溢出，破坏内存，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer JavaScript 整数溢出代码执行漏洞、Microsoft Internet Explorer 远程代码执行漏洞、Microsoft Office 内存破坏远程代码执行漏洞、Microsoft Visio Viewer VSD 文件格式远程代码执行漏洞（CNVD-2012-13629）、Microsoft Windows 本地权限提升漏洞、Microsoft Windows 远程管理协议远程堆缓冲区溢出漏洞、Microsoft Windows 通用控件 ActiveX 控件远程代码执行漏洞、Microsoft Internet Explorer 虚函数表远程代码执行漏洞等。上述漏洞的综合评级均为“高危”，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=53438
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53437
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53441
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53443
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53445
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53447
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53444
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53440

2、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，Adobe 产品被披露存在多个安全漏洞，攻击者可利用漏洞构建恶意 PDF 文件，诱使用户解析，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 内存破坏漏洞（CNVD-2012-13644）、Adobe Flash Player 远程代码执行漏洞（CNVD-2012-13645）、Adobe Acrobat/Reader 内存破坏漏洞（CNVD-2012-13643）、Adobe Acrobat/Reader 远程缓冲区溢出漏洞（CNVD-2012-13639）、Adobe Acrobat/Reader 远程缓冲区溢出漏洞（CNVD-2012-13638）、Adobe Acrobat/Reader 远程缓冲区溢出漏洞（CNVD-2012-13640）、Adobe Acrobat/Reader 内存破坏漏洞（CNVD-2012-13642）、Adobe Flash Player 存在未明执行代码漏洞等。上述漏洞的综合评级均为“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=53458
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53459
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53457
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53453

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53452

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53454

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53456

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53429

3、ownCloud 安全漏洞

ownCloud 是一款开源的个人云服务端软件。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞通过诱使管理员用户登陆恶意网址，通过读取或写入某些特定构造的 APP 参数值或软件清单，进而在用户浏览器中注入执行恶意脚本代码。

CNVD 收录的相关漏洞包括：ownCloud 跨站请求伪造漏洞、ownCloud 任意文件读取/写入漏洞、ownCloud 脚本注入漏洞（CNVD-2012-13614）、ownCloud 'token'参数跨站脚本漏洞、ownCloud 文件修改漏洞、ownCloud 脚本注入漏洞（CNVD-2012-13615）、ownCloud 跨站脚本漏洞。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=53419

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53421

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53423

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53420

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53418

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53424

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53422

4、HP 产品安全漏洞

HP Integrity Server 是一款惠普公司推出的服务器；HP Service Manager 是一款帮助用户迅速部署一个全面的 IT 服务管理的解决方案；HP Fortify Software Security Center 是一套自动化和管理企业应用安全的产品。本周，上述产品被披露存在多个漏洞，攻击者利用漏洞发起拒绝服务攻击，执行任意代码。

CNVD 收录的相关漏洞包括：HP Service Manager 和 Service Center 拒绝服务漏洞、HP Service Manager 和 Service Center 跨站脚本漏洞、HP Fortify Software Security Center 信息泄露漏洞（CNVD-2012-13616）、HP Fortify Software Security Center 信息泄露漏洞（CNVD-2012-13617）、HP Integrity Servers 多个模块存在未明拒绝服务漏洞。其中，“HP Service Manager 和 Service Center 拒绝服务漏洞”的综合评级为“高危”，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=53428

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53427

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53425

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53426

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53388

5、Spytech NetVizor 远程缓冲区溢出漏洞

Spytech NetVizor 是一款网络监控软件。本周，Spytech NetVizor 被披露存在一个综合评级为“高危”的缓冲区溢出漏洞。由于未能正确处理用户提交的请求，攻击者利用漏洞进行缓冲区溢出攻击，使应用程序崩溃或执行任意代码。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=53380

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-2012-13558	Linux kernel NCI 远程栈缓冲区溢出漏洞	高	用户可参考如下第三方补丁程序： http://marc.info/?l=linux-kernel
CNVD-2012-13579	Cyclope Employee Surveillance Solution 'username' SQL 注入漏洞	高	暂无
CNVD-2012-13562	Joomla! RSGallery2 组件 SQL 注入漏洞	高	Joomla! RSGallery2 3.2.0 或 2.3.0 已经修复此漏洞，建议用户下载使用： http://joomlancode.org/gf/download/frs_release/17326/75428/com_rsgallery2_3.2.0.zip
CNVD-2012-13588	Tunnelblick 存在多个本地权限提升漏洞	高	暂无
CNVD-2012-13583	TCEexam 存在多个 SQL 注入漏洞	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.tcexam.org
CNVD-2012-13605	ProQuiz 'username' POST 参数 SQL 注入漏洞	高	暂无
CNVD-2012-13584	Siemens COMOS 存在未明安全绕过漏洞	高	厂商已修复此漏洞，建议用户下载使用： http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-312568.pdf
CNVD-2012-13585	WordPress 插件 Mz-jajak 'id' SQL 注入漏洞	高	暂无

CNVD-2012-13602	Hotel Booking Portal 存在多个 SQL 注入漏洞	高	暂无
CNVD-2012-13601	ProQuiz SQL 注入漏洞	高	暂无
CNVD-2012-13591	Amazon Kindle Touch libkindleplugin 脚本浏览器插件漏洞（CNVD-2012-13591）	高	建议用户升级使用： http://www.amazon.com/Kindle-Touch-e-Reader-Touch-Screen-Wi-Fi-Special-Offers/dp/B005890G8Y

表 3 部分高危漏洞列表

小结：本周，Microsoft、Adobe、HP 的多个产品被披露存在多个安全漏洞，攻击者发起拒绝服务攻击或执行脚本代码获得主机操作系统管理权限。ownCloud 作为一款云服务端软件也被披露存在多个漏洞，使得大量的云端用户主机操作系统受到关联威胁。此外，网络监控软件 Spytech NetVizor 被披露存在零日漏洞，对网络服务器系统管理安全构成威胁，相关用户需加强防范。

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、IBM 发布升级程序，修补多款产品安全漏洞

IBM Lotus Sametime Server 是一款实时协作和网络会议解决方案。IBM WebSphere MQ 是一款用于在企业中提供消息传输服务的解决方案。本周，IBM 发布升级程序，修补了多款产品存在的漏洞。攻击者可以利用漏洞绕过安全限制，下载文件或以目标用户上下文执行任意管理操作。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=19778
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=19777
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=19851

本周要闻速递

1. 苹果回应 iOS 短信漏洞

近日，一位法国黑客发现了 iOS 系统短信功能的一个漏洞，该漏洞使垃圾信息发布者可以伪装成合法号码，这可能导致欺诈或用户个人信息泄露。苹果一名发言人表示，用户可以通过使用 iMessage 消息服务来规避这一问题。当使用 iMessage 替代短信时，地址将得到验证，从而避免这样的欺诈攻击。短信的一个限制在于，信息地址可以被伪装。因此我们提醒用户，当被短信重定向至未知网站或地址时，应当保持警惕。”实际

上，非 iPhone 用户也可能遭遇这样的问题。许多服务都可以帮助短信发送者伪装身份，而无论短信接收者使用的是什么手机、操作系统和运营商服务。用户在打开来自短信的网址时都应当谨慎。

参考链接：<http://tech.sina.com.cn/s/2012-08-19/08427521652.shtml>

2. 微软多个产品存在高危漏洞

周三凌晨，微软发布 8 月安全补丁公告，此次漏洞公告修复涉及 Windows7、Office 系列和多个微软其他产品。其中对网民威胁最大的是 Office 产品的高危漏洞，一旦被黑客攻击，用户打开攻击者恶意构造的 Office 文档，恶意文档中内嵌的木马就会被执行。此次针对 Microsoft Office 高危漏洞的更新补丁，修复的重点是高危的远程执行代码漏洞，以避免攻击者轻易获得与当前用户相同的用户权限。这并非近期 Office 被公开披露的第一个漏洞，微软在 7 月份发布的安全报告中就已针对 Microsoft Office for Mac 中对用户权限造成极大威胁的漏洞进行过修复。

参考链接：<http://digi.hsw.cn/system/2012/08/17/051431244.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