

信息安全漏洞周报

2012 年 8 月 20 日-2012 年 8 月 26 日

2012 年第 34 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 122 个，其中高危漏洞 46 个、中危漏洞 65 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 116 个。本周收录的漏洞中，已有 79 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“Mozilla Firefox 远程拒绝服务漏洞”、“Divx Player 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 6 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 122 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，网御星云公司及一位个人报送者向 CNVD 共提交了 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	86	0
绿盟科技	87	0
安天实验室	60	0
恒安嘉新	29	0
天融信	25	0
安氏领信	7	0
网御星云	1	1
个人报送者	1	1
报送总计	296	2

录入总计	122（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 McAfee、Adobe、HP、SAP 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	McAfee	19	16%
2	Adobe	10	8%
3	HP	8	7%
4	SAP	5	4%
5	IBM	4	3%
6	Apache	4	3%
7	Drupal	4	3%
8	WordPress	2	2%
9	Oracle	2	2%
10	Mozilla	1	1%
11	其它	63	51%

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 122 个漏洞。其中操作系统漏洞 6 个，应用程序漏洞 66 个，WEB 应用漏洞 25 个，网络设备漏洞 3 个，安全产品漏洞 18 个，数据库漏洞 4 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	6
应用程序漏洞	66
WEB 应用漏洞	25
网络设备漏洞	3
数据库漏洞	4
安全产品漏洞	18

表 3 漏洞按影响类型统计表

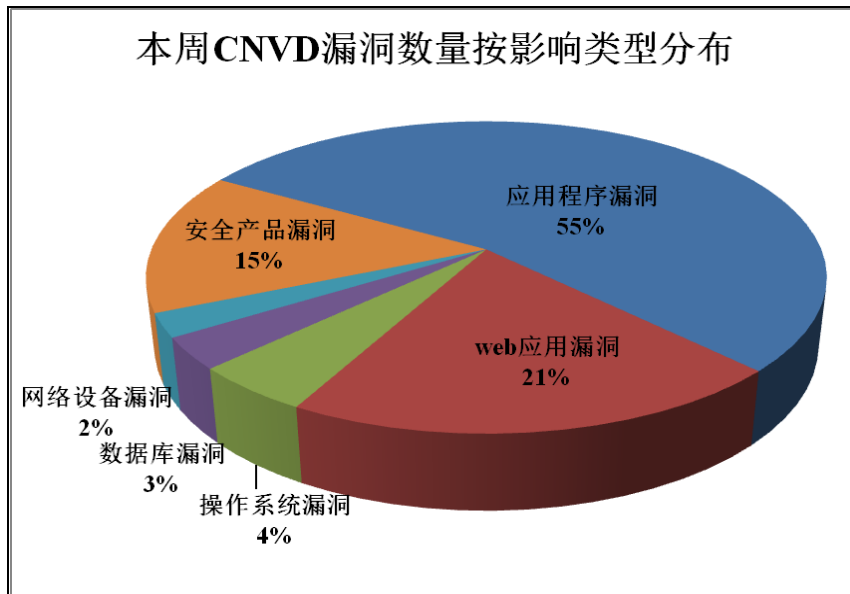


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 3 个网络设备漏洞：“ALPHA Networks ADSL Wireless Router 'returnJSON.htm'管理员密码泄露漏洞、Korenix Jetport 和 ORing 默认密码漏洞、Tor 未初始化内存读取漏洞”。其中，“ALPHA Networks ADSL Wireless Router 'returnJSON.htm'管理员密码泄露漏洞”和“Korenix Jetport 和 ORing 默认密码漏洞”的综合评级均为“高危”。

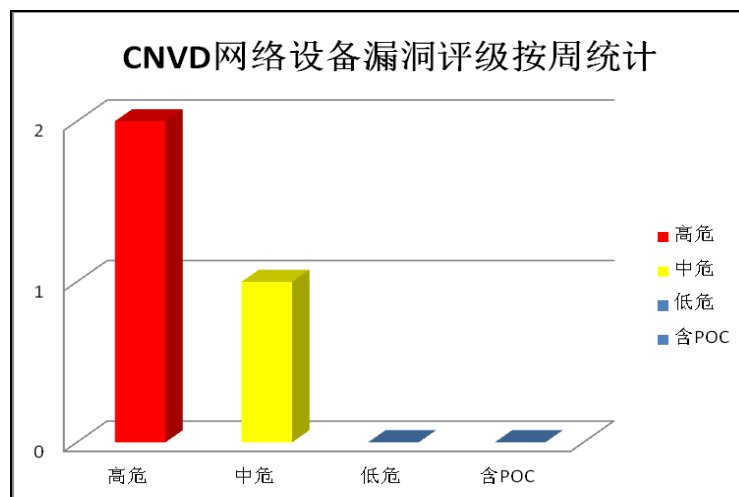


图 2 网络设备漏洞统计

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、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序；Adobe Shockwave Player 是用于播放 Director Shockwave Studio 网页的插件。本周，上述 Adobe 产品被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Adobe Flash Player/AIR 整数溢出漏洞、Adobe Flash Player/AIR 存在未明漏洞（CNVD-2012-13723、CNVD-2012-13725、CNVD-2012-13721、CNVD-2012-13719）、Adobe Shockwave Player 远程内存破坏漏洞（CNVD-2012-13676、CNVD-2012-13690、CNVD-2012-13691）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=53861
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53858
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53860
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53856
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53837
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53515
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53656
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53657

2、IBM 产品安全漏洞

IBM Lotus Domino 服务器是一款基于 WEB 合作的应用程序架构。本周，该产品被披露存在多个安全漏洞，攻击者可利用漏洞获得敏感信息或劫持用户会话。

CNVD 收录的相关漏洞包括：IBM Lotus Domino HTTP 应答分片漏洞、IBM Lotus Domino 跨站脚本漏洞（CNVD-2012-13698、CNVD-2012-13697）。其中，“IBM Lotus Domino HTTP 应答分片漏洞”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=53697
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53696
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53695

3、SAP 产品安全漏洞

SAP Business Objects Financial Consolidation 是一款企业绩效管理产品；SAP Crystal Reports Server 是一款报表解决方案产品，主要通过网络或嵌入企业应用程序来创建、管理和交付报表；SAP NetWeaver 是一款 SAP 业务套件解决方案产品。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执行任意代码。

CNVD 收录的相关漏洞包括：SAP Business Objects Financial Consolidation 'CtAppReg.dll'远程代码执行漏洞、SAP Crystal Reports 'ebus-3-3-2-7.dll'远程代码执行漏洞、

SAP Netweaver 'SAPHostControl'服务远程代码执行漏洞。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=53636
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53637
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53638

4、HP 产品安全漏洞

HP Serviceguard 是惠普针对 HP-UX 和 Linux 操作系统提供的应用程序保护解决方案；Hewlett-Packard Virtual SAN Appliance 则是用于转换服务器磁盘驱动器和外部原有存储到虚拟 iSCSI SAN 的软件产品。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，执行任意命令。

CNVD 收录的相关漏洞包括：HP Serviceguard 存在未明拒绝服务漏洞、HP SAN/iQ 任意 SHELL 命令执行漏洞、HP SAN/iQ 未文档化账户漏洞。上述漏洞的综合评级均为“高危”，其中，厂商已经修复了“HP Serviceguard 存在未明拒绝服务漏洞”。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=53701
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53702
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53536

5、Mozilla Firefox 远程拒绝服务漏洞

Mozilla Firefox 是一款开源的 WEB 浏览器。本周，Mozilla Firefox 被披露存在一个远程拒绝服务漏洞。由于 Mozilla Firefox 未能正确处理特制的 HTML 代码，攻击者可以利用漏洞构建恶意 WEB 页，诱使用户解析，使应用程序崩溃。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=53716

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-2012-13742	ClipBucket SQL 注入漏洞 (CNVD-2012-13742)	高	暂无
CNVD-2012-13683	xmlsd 'xmlsd_chardata()'单字节 错误缓冲区溢出漏洞	高	xmlsd 0.9.0 已经修复此漏洞，建议用户下载使用： https://opensource.conformal.com/

CNVD-2012-13735	Rugged 操作系统私钥泄露漏洞	高	暂无
CNVD-2012-13682	McAfee SmartFilter 'SFAdminSrv.exe'远程代码执行漏洞	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://www.zerodayinitiative.com/advisories/ZDI-12-140
CNVD-2012-13728	Korenix Jetport 和 ORing 默认密码漏洞	高	暂无
CNVD-2012-13707	WordPress 插件 Zingiri Web Shop SQL 注入漏洞	高	WordPress 插件 Zingiri Web Shop 2.4.8 版本已修复此漏洞，建议用户下载使用： http://wordpress.org/extend/plugins/zingiri-web-shop/
CNVD-2012-13705	w-Agora SQL 注入漏洞	高	暂无
CNVD-2012-13715	YourArcadeScript 'id' SQL 注入漏洞	高	暂无
CNVD-2012-13700	ALPHA Networks ADSL Wireless Router 'returnJSON.htm' 管理员密码泄露漏洞	高	暂无
CNVD-2012-13678	GIMP 远程命令执行漏洞（CNVD-2012-13678）	高	暂无
CNVD-2012-13680	Inferno vBShout 'infernoshout.php' SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，HP、SAP、IBM 的多个应用或服务器产品被披露存在多个安全漏洞，攻击者利用漏洞可发起拒绝服务攻击或执行任意代码，严重的取得系统管理权限。此外，Adobe、Mozilla 的桌面应用程序、浏览器等产品被披露存在高危漏洞或零日漏洞，由于产品用户群体广泛，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、Novell 发布升级程序，修补 eDirectory 安全漏洞

Novell eDirectory 是一款跨平台的目录服务器。本周，Novell 发布升级程序，修补了 eDirectory 存在的漏洞。攻击者可以利用漏洞触发栈缓冲区溢出，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=20591

本周要闻速递

1. iPhone 短信漏洞不影响其他系统

据国外媒体报道,本月初,iPhone 爆出短信安全漏洞。从目前来看,该漏洞似乎仅涉及 iOS 系统。移动安全公司 AdaptiveMobile 称,相较其他移动系统用户,iPhone 用户更加难以辨认出诈骗短信和钓鱼攻击。事实上,iOS 为短信接收者显示“回复至”号码,诈骗分子可以修改该号码,以用于不法目的。苹果公司并未对短信漏洞发表评论,但苹果公司指出,如果用户使用 iMessage (认证 iOS 设备互发信息),那么就不会存在任何问题。

参考链接: <http://www.newhua.com/2012/0827/174119.shtml>

2. 黑客利用 Adobe Flash 漏洞

黑客利用电子邮件夹带含有恶意 Flash 内容的 Word 文件,里面所含的 ActionScript 会使用 Heap Spraying 技术嵌入 shellcode,借 Flash 漏洞进行攻击。由于电子邮件夹带的 Word 文件的标题多为 iPhone 5、伦敦奥运等热门议题,诱使不少使用者开启该文档。根据赛门铁克的统计,自 8/10 发现至 8/21 截止,总共拦截 1300 次攻击,电子邮件的高峰在 8/13 日。根据 Adobe 的资安通报显示,主要攻击目标是使用微软 Internet Explorer 浏览器的 Windows 系统,不过 Windows、OS X、Linux 及 Android 各平台的 Flash 播放程序均含有此漏洞,如果遭受攻击,设备可能当机或黑客控制。Adobe 在上周(8/14)发布定期更新,修补 Acrobat/Reader、Flash 播放程序与 Shockwave 播放程序等软件。周二(8/21)又推出 Flash 播放程序的紧急更新,并呼吁各平台使用者均应更新,尤其是 Windows 平台的修复优先次序评估为一,代表使用者应在 72 小时内更新完毕。

参考链接: <http://news.qudong.com/soft/shadu/20120825/122161.html>

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