

信息安全漏洞周报

2012 年 8 月 27 日-2012 年 9 月 2 日

2012 年第 35 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**高**。

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 143 个，其中高危漏洞 67 个、中危漏洞 69 个、低危漏洞 7 个。上述漏洞中，可利用来实施远程攻击的漏洞有 134 个。本周收录的漏洞中，已有 108 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“Microsoft Indexing Service 'ixsso.dll' ActiveX 控件拒绝服务漏洞”、“Java JRE 任意代码执行漏洞”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 143 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、天融信等单位报送数量较多。此外，网御星云、安恒公司及一位个人报送者向 CNVD 共提交了 8 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	153	0
启明星辰	115	0
安天实验室	30	0
恒安嘉新	10	0
天融信	33	0
安氏领信	7	0
网御星云	4	4
安恒	1	1

个人报送者	3	3
报送总计	356	8
录入总计	143（去重）	8

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、HP、Symantec、IBM 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	Mozilla	32	22%
2	HP	11	8%
3	Symantec	6	4%
4	IBM	5	3%
5	Atlassian	5	3%
6	WordPress	4	3%
7	Linux	4	3%
8	Novell	2	2%
9	Microsoft	1	1%
10	Oracle	1	1%
11	其它	72	50%

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 143 个漏洞。其中操作系统漏洞 5 个，应用程序漏洞 108 个，WEB 应用漏洞 20 个，网络设备漏洞 8 个，安全产品漏洞 1 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	5
应用程序漏洞	108
WEB 应用漏洞	20
网络设备漏洞	8
数据库漏洞	1
安全产品漏洞	1

表 3 漏洞按影响类型统计表

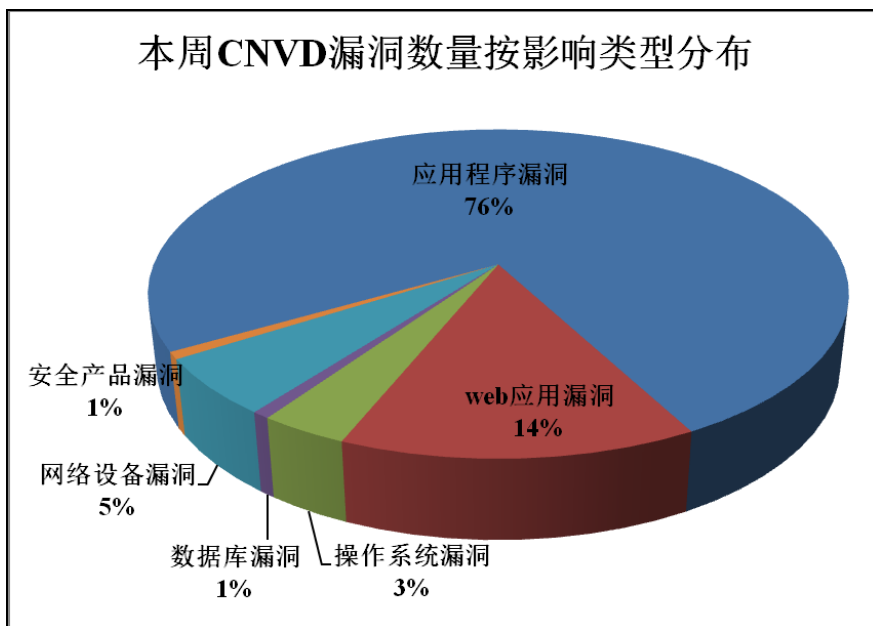


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 8 个网络设备漏洞：“Tor 拒绝服务漏洞、Tor 信息泄露漏洞、Symantec Messaging Gateway 信息泄露漏洞（CNVD-2012-13841）、Symantec Messaging Gateway 跨站请求伪造漏洞（CNVD-2012-13839）、Symantec Messaging Gateway 安全绕过漏洞（CNVD-2012-13840）、Symantec Messaging Gateway 跨站脚本漏洞（CNVD-2012-13842）、Symantec Messaging Gateway SSH 默认密码安全绕过漏洞、GarrettCom Magnum MNS-6K 软件硬编码密码安全绕过漏洞”。其中，“Symantec Messaging Gateway 跨站请求伪造漏洞（CNVD-2012-13839）、Symantec Messaging Gateway 安全绕过漏洞（CNVD-2012-13840）、Symantec Messaging Gateway 跨站脚本漏洞（CNVD-2012-13842）、Symantec Messaging Gateway SSH 默认密码安全绕过漏洞、GarrettCom Magnum MNS-6K 软件硬编码密码安全绕过漏洞”的综合评级均为“高危”。

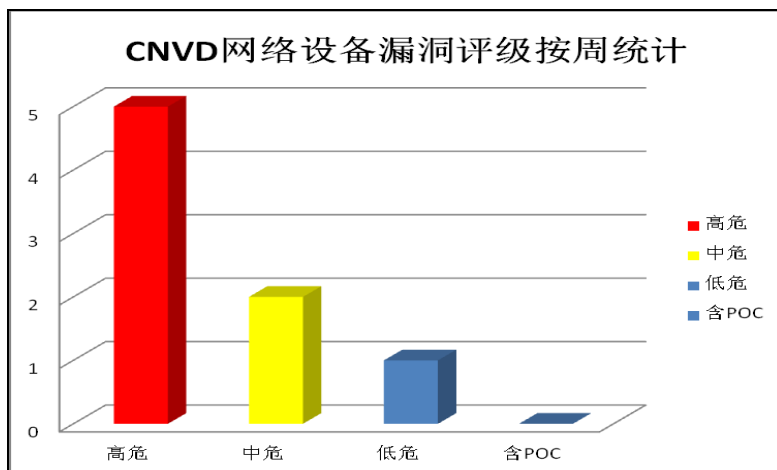


图 2 网络设备漏洞统计

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、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 Mozilla 产品被披露存在多个安全漏洞，攻击者利用漏洞可提升特权、远程调试服务，泄露敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox/SeaMonkey/Thunderbird 内存错误引用漏洞（CNVD-2012-13864）、Mozilla Firefox/SeaMonkey/Thunderbird 内存破坏漏洞（CNVD-2012-13865）、Mozilla Firefox about:newtab 权限提升漏洞、Mozilla Firefox about:newtab 权限提升漏洞、Mozilla Firefox/SeaMonkey/Thunderbird SVG 缓冲区溢出漏洞、Mozilla Firefox HTTPMonitor 访问漏洞、Mozilla Firefox/SeaMonkey/Thunderbird location 对象安全绕过漏洞、Mozilla Firefox/Thunderbird Web console eval 权限提升漏洞等。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=55115
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55116
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55216
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55235
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55240
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55244
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55255
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55275

2、Symantec 产品安全漏洞

Symantec Messaging Gateway（此前曾用名称 Brightmail Gateway Small Business Edition）是一款电子邮件病毒防护硬件设备。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可绕过安全限制执行未授权操作，获得敏感信息，或对系统进行进一步攻击。

CNVD 收录的相关漏洞包括：Symantec Messaging Gateway 信息泄露漏洞（CNVD-2012-13841）、Symantec Messaging Gateway 安全绕过漏洞（CNVD-2012-13840）、Symantec Messaging Gateway 跨站请求伪造漏洞（CNVD-2012-13839）、Symantec Messaging Gateway 跨站脚本漏洞（CNVD-2012-13842）、Symantec Messaging Gateway SSH 默认密码安全绕过漏洞。其中，除“Symantec Messaging Gateway 信息泄露漏洞（CNVD-2012-13841）”，其余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=54895
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=54875
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=54896
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=54897
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=54899

3、HP 产品安全漏洞

HP SiteScope 是一款为提供 IT 基础部件可用性和性能监视的解决方案；HP Operations Orchestration 是一款运维手册自动化平台，提供客户端设备和数据中心基础设施变更、部署功能；HP Intelligent Management Center 是普公司发行的一款惠应用智能管理程序。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可更新管理员验证凭据，执行任意代码。

CNVD 收录的相关漏洞包括：HP SiteScope SOAP update 调用任意代码执行漏洞、HP SiteScope UploadFilesHandle 目录遍历漏洞、HP SiteScope SOAP getSiteScopeConfiguration 调用任意文件获取漏洞、HP SiteScope SOAP loadFileContent 调用任意文件获取漏洞、HP SiteScope SOAP getFileInternal 调用任意文件获取漏洞、HP SiteScope SOAP create 调用账户添加漏洞、HP Operations Orchestration 'RSScheduler Service JDBC Connector'远程代码执行漏洞、HP Intelligent Management Centre 'uam.exe' 栈缓冲区溢出漏洞等。上述漏洞的综合评级均为“高危”。目前，厂商尚未提供修复程序，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=55335
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55337
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55319
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55321
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55318
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55316
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55315
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55296

4、Linux 安全漏洞

Linux 是一款开源的操作系统。本周，Linux 系统被披露存在多个漏洞，攻击者利用漏洞可提升权限，触发内核崩溃，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Linux i.MX 时钟拒绝服务漏洞、Linux 目录树删除拒绝服务漏洞、Linux Kernel 拒绝服务漏洞（CNVD-2012-13819）、Linux Kernel 存在多个缓冲区溢出漏洞。其中，“Linux Kernel 拒绝服务漏洞（CNVD-2012-13819）”和“Linux Kernel 存在多个缓冲区溢出漏洞”的综合评级均为“高危”。厂商已经修复上述漏洞。

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=55055
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=55037
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=54696
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=54715

5、Microsoft Indexing Service 'ixss.dll' ActiveX 控件拒绝服务漏洞

Microsoft windows 是一款流行的操作系统。本周，Microsoft windows 被披露存在一个综合评级为“高危”的远程拒绝服务漏洞。由于 Microsoft windows Indexing Service Server-side (ixss.dll)存在空指针引用错误，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=54536

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-2012-13898	Atlassian Bamboo OGNL 表达式注入漏洞	高	厂商已经修复此漏洞，建议用户下载使用： https://confluence.atlassian.com/display/BAMBOO/Bamboo Security Advisory 2012-08-28
CNVD-2012-13832	Tunnelblick 系统调用权限提升漏洞	高	暂无
CNVD-2012-13911	Novell ZENWorks AdminStudio 'ISGrid.dll' Activex 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-12-180/
CNVD-2012-13834	CommPort 'signup.cgi' SQL 注入漏洞	高	暂无
CNVD-2012-13855	EMC Cloud Tiering Appliance (CTA)验证绕过漏洞	高	注册用户可联系供应商获得相应的补丁程序： https://support.emc.com/products/6298 https://support.emc.com/products/1678
CNVD-2012-13847	Vlinks 'id' SQL 注入漏洞	高	暂无

CNVD-2012-13845	SysAid 存在未明 SQL 注入漏洞	高	SysAid 8.5.08 已经修复此漏洞，建议用户下载使用： http://www.sysaid.com/bugs-fixed-8-5.htm
CNVD-2012-13822	McAfee Virtual Technician 任意代码执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://kc.mcafee.com/corporate/index?page=content
CNVD-2012-13801	elcomCMS 'UploadStyleSheet.aspx'任意文件上传漏洞	高	Elcom Community Manager 7.5 已经修复此漏洞，建议用户下载使用： http://www.elcomcms.com
CNVD-2012-13824	Banana Dance SQL 注入漏洞	高	用户可联系供应商获得补丁信息： http://www.bananadance.org
CNVD-2012-13821	Mesa 'visit_field()'缓冲区溢出漏洞	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.mesa3d.org

表 3 部分高危漏洞列表

小结：本周，Mozilla、Symantec、HP 的多个应用或服务器产品被披露存在多个安全漏洞，攻击者利用漏洞可提升特权、泄露敏感信息、执行任意代码。此外，Linux、Microsoft windows 操作系统也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。

除上述高危漏洞外，本周 CNVD 紧急发布了两个安全公告，对 Oracle JRE 1.7 以及 Iphone iOS 系统的两个中危 0day 漏洞进行预警。CNVD 成员单位 360 公司以及国内安全企业对 Oracle JRE 1.7 远程代码执行漏洞（CNVD-2012-13827）影响情况进行了监测，发现有攻击者已经在利用该漏洞发起挂马攻击。

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、Dell 发布升级程序，修补 Crowbar Ohai 插件漏洞

本周，Dell 发布升级程序，修补了 Crowbar Ohai 插件存在的漏洞。本地攻击者可以利用漏洞以 ROOT 权限执行任意命令。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=20893

本周要闻速递

OS X 平台的 Java 7 漏洞补丁已发布

据悉，有安全专家发现 Java 7 运行环境再次出现漏洞，并通知 Mac 用户提高警惕，因为漏洞能够让攻击者通过各种浏览器对安装 Java 的设备进行攻击。本次消息公布之后，甲骨文很快做出了调整，发布了针对 Java 7 的漏洞补丁。据甲骨文的官方消息透露，新补丁不仅仅修复了几天之前发现的 Java 7 重大漏洞，同时还解决了其它的一些小问题，并提高了系统的稳定性。另外，甲骨文还同时发布了 Java SE 6 的更新，在修复漏洞的同时也为用户带来了更良好的运行环境。目前 Java 7 的漏洞补丁和 Java SE 6 均已在甲骨文的 Java 页面提供下载。

参考链接：<http://tech.sina.com.cn/s/2012-08-31/10377569084.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