

信息安全漏洞周报

2012 年 7 月 16 日-2012 年 7 月 22 日

2012 年第 29 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 131 个，其中高危漏洞 53 个、中危漏洞 74 个、低危漏洞 4 个。上述漏洞中，可利用来实施远程攻击的漏洞有 126 个。本周收录的漏洞中，已有 91 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“Telnet FTP Server 'PASV'命令远程内存破坏漏洞”、“Snack Sound Toolkit 'GetWavHeader()'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 131 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、恒安嘉新、天融信、安天实验室等单位报送数量较多。此外，恒安嘉新、杭州安恒等公司以及个人漏洞研究者向 CNVD 提交了 11 个原创漏洞或漏洞事件。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	109	0
启明星辰	84	0
安天实验室	34	0
恒安嘉新	26	3
天融信	26	0
安氏领信	10	0
知道创宇	7	0
个人报送者	3	3
杭州安恒信息技术有	5	5

限公司		
报送总计	304	11
录入总计	131（去重）	11

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、Moodle、libexif、Cisco 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	Mozilla	19	15%
2	Moodle	10	8%
3	libexif	8	6%
4	Cisco	6	5%
5	DotNetNuke	4	3%
6	IBM	4	3%
7	HP	3	2%
8	Oracle	3	2%
9	RSA	3	2%
10	Red Hat	2	1%
11	其它	69	53%

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 131 个漏洞。其中操作系统漏洞 2 个，应用程序漏洞 90 个，WEB 应用漏洞 26 个，数据库漏洞 3 个，网络设备漏洞 10 个。本周末收录安全产品类型的漏洞。

漏洞影响对象类型	漏洞数量
操作系统漏洞	2
应用程序漏洞	90
WEB 应用漏洞	26
网络设备漏洞	10
数据库漏洞	3
安全产品漏洞	0

表 3 漏洞按影响类型统计表

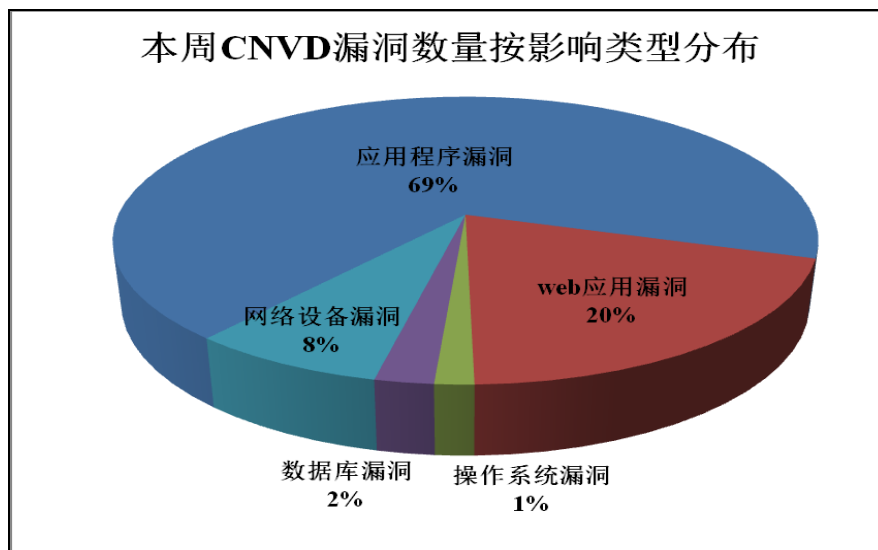


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 10 个网络设备漏洞。其中，“Cisco TelePresence Immersive Endpoint Devices 远程命令注入漏洞（CNVD-2012-13002）、Cisco TelePresence Immersive Endpoint Devices 远程命令注入漏洞（CNVD-2012-13005）、Cisco TelePresence Recording Server WEB 接口远程命令注入漏洞、Cisco TelePresence 畸形 IP 报文拒绝服务漏洞、Cisco TelePresence Cisco 发现协议远程代码执行漏洞、SMC Networks SMC8024L2 交换机 WEB 接口验证绕过漏洞、EMC 多个产品安全绕过漏洞”的综合评级均为“高危”，“TP Link 网关多个 HTML 代码注入漏洞、Johnson Controls 多个产品远程命令执行漏洞、Vivotek Network Cameras 信息泄露漏洞”的综合评级均为“中危”。目前，互联网上已经出现了针对“Vivotek Network Cameras 信息泄露漏洞”的攻击代码。

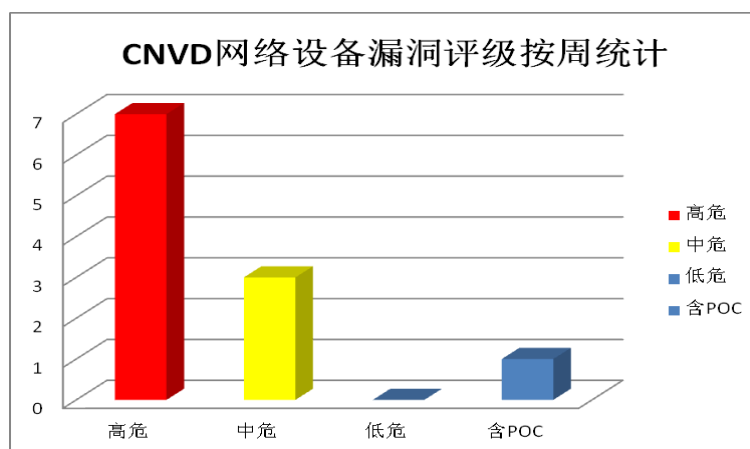


图 2 网络设备漏洞统计



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、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，攻击者利用漏洞可使应用程序崩溃，触发堆缓冲区溢出或执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird/SeaMonkey 越界读漏洞（CNVD-2012-13111）、Mozilla Firefox/Thunderbird/SeaMonkey 类型转换漏洞（CNVD-2012-13110）、Mozilla Firefox/Thunderbird/SeaMonkey 内存错误引用漏洞（CNVD-2012-13108）、Mozilla Firefox/Thunderbird/SeaMonkey 权限提升漏洞（CNVD-2012-13095）、Mozilla Firefox/Thunderbird/Seamonkey 内存破坏漏洞（CNVD-2012-13092）、Mozilla Firefox/Thunderbird/SeaMonkey 内存破坏漏洞（CNVD-2012-13101）、Mozilla Firefox/Thunderbird/SeaMonkey 内存错误引用漏洞（CNVD-2012-13099）、Mozilla Firefox/Thunderbird/Seamonkey 内存破坏漏洞（CNVD-2012-13090）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=52078
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52087
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52089
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52080
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52083
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52096
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52098
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52099

2、Cisco 产品安全漏洞

Cisco TelePresence Immersive Endpoint 是一款视频系统软件；Cisco Linksys PlayerPT ActiveX 是一款绑定在 Cisco WVC200 Wireless-G PTZ Internet Video Camera 产品中的插件，可使用户通过 IE 查看功能界面。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可发起拒绝服务攻击，以高特权执行任意系统命令。

CNVD 收录的相关漏洞包括：Cisco Linksys PlayerPT ActiveX Control 'SetSource()' 缓冲区溢出漏洞、Cisco TelePresence Immersive Endpoint Devices 远程命令注入漏洞（CNVD-2012-13005）、Cisco TelePresence Immersive Endpoint Devices 远程命令注入漏洞（CNVD-2012-13002）、Cisco TelePresence Recording Server WEB 接口远程命令注入漏洞、Cisco TelePresence 畸形 IP 报文拒绝服务漏洞。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=51819
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51816
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51797
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51821
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51800
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52081

3、IBM 产品安全漏洞

IBM DB2 Universal Database Server 是一款大型的商业关系数据库系统；IBM Lotus Protector for Mail Security 是一款提供垃圾邮件保护和控制的解决方案。本周，上述 IBM 产品被披露存在多个安全漏洞，攻击者利用漏洞可获取敏感文件信息；发起栈缓冲区溢出攻击。

CNVD 收录的相关漏洞包括：IBM DB2 敏感信息泄露漏洞、IBM DB2 缓冲区溢出漏洞、IBM DB2 JAR 文件替换漏洞、IBM Lotus Protector for Mail Security 存在多个安全漏洞。其中，“IBM DB2 缓冲区溢出漏洞”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=52033
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52035
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52038
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52042

4、Moodle 安全漏洞

Moodle 是一款开源的网络教学应用软件。本周，Moodle 被披露存在多个漏洞。攻击者利用漏洞绕过安全限制，访问受限文件，获得敏感信息或劫持用户会话，获得数据库信息或控制应用系统。

CNVD 收录的相关漏洞包括：Moodle Feedback 模块 SQL 注入漏洞、Moodle LDAP 验证不安全协议重定向漏洞、Moodle 论坛订阅验证漏洞、Moodle 敏感信息访问漏洞、Moodle 受限文件访问漏洞、Moodle LTI 跨站脚本漏洞、Moodle 安全限制漏洞、Moodle 文件大小上传限制绕过漏洞。其中，“Moodle Feedback 模块 SQL 注入漏洞”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=52043
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52044
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52030

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52032

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52034

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52036

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52037

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52040

5、Telnet FTP Server 'PASV'命令远程内存破坏漏洞

Telnet FTP Server 是一款 FTP 服务软件。本周，Telnet FTP Server 被披露存在一个综合评级为“高危”的内存破坏漏洞。由于 Telnet FTP Server 未能正确处理用户提交的请求，远程攻击者可以利用漏洞提交恶意请求使服务程序崩溃。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=51936

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-2012-13096	HP StorageWorks File Migration Agent 'RsaCIFS.dll'栈缓冲区溢出漏洞	高	暂无
CNVD-2012-13065	libjpeg-turbo 'get_sos()' JPEG Decompression 缓冲区溢出漏洞	高	libjpeg-turbo 1.2.1 版本已修复此漏洞，建议用户下载使用： http://www.libjpeg-turbo.org/
CNVD-2012-13067	Beyond Security beSTORM 'WinGraphviz.dll' ActiveX 控件堆缓冲区溢出漏洞	高	暂无
CNVD-2012-13057	WebPagetest 文件上传漏洞	高	WebPagetest 2.7.1 版本已修复此漏洞，建议用户下载使用： http://www.webpagetest.org/
CNVD-2012-13066	WordPress 插件 Resume Submissions 和 Job Postings 任意文件上传漏洞	高	暂无
CNVD-2012-13023	EMC 多个产品安全绕过漏洞	高	厂商已经修复此漏洞，建议用户下载使用： http://www.emc.com/
CNVD-2012-13060	Elite Bulletin Board 存在多个 SQL 注入漏洞	高	暂无
CNVD-2012-13022	Eucalyptus VMware Broker 验证绕过漏洞	高	Eucalyptus 3.0.2 或 3.0.1 已经修复此漏洞，建议用户下载使用： http://www.eucalyptus.com

CNVD-2012-13084	EGallery uploadify.php 任意文件上传漏洞	高	暂无
CNVD-2012-13015	SMC Networks SMC8024L2 交换机 WEB 接口验证绕过漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Mozilla 的多款产品被披露存在多个漏洞，攻击者利用漏洞使应用程序崩溃，触发堆缓冲区溢出，执行任意代码。Cisco 的两款产品也被披露存在多个漏洞，利用漏洞可发起拒绝服务攻击，以高特权执行任意系统命令。IBM 产品存在的漏洞，可导致栈缓冲区溢出，泄露敏感文件信息。上述软件产品对终端用户桌面应用安全以及企业业务系统安全构成较大威胁。

此外，Moodle 网络教学应用程序存在的漏洞可被攻击者利用以绕过安全限制，访问受限文件，获得敏感信息或劫持用户会话，获得数据库信息或控制应用系统。Telnet FTP Server 服务程序被披露存在零日漏洞。上述漏洞对特定用户或网络服务器安全构成威胁，管理员需加强防范。

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、EMC 发布升级程序，修补多款产品安全漏洞

EMC Celerra Network Server 实施各种安全功能来控制用户和网络访问、监视系统访问；EMC VNX 是 EMC 公司推出的统一存储系统。本周，EMC 发布升级程序，修补了多款产品存在的漏洞。允许攻击者利用漏洞绕过安全限制，获得对输出文件系统的未授权访问。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=18836

本周要闻速递

1. 视频会议有泄密风险 思科紧急补漏洞

思科在官方网站上宣布，旗下高端网真产品线的软件有漏洞，包括 Cisco TelePresence Recording Server、TelePresence Manager、TelePresence Multipoint Switch、TelePresence Immersive Endpoint System 等产品，都可能因为这次所发现的软件漏洞，而让有心人士未经授权就可远端操控视频会议软件，甚至窃取视频内容来得知企业机密。思科也紧急推出修复补丁。企业只要安装更新补丁，就可以避免因为网真产品的漏洞，而引

发各种网络安全问题。

参考链接: <http://network.chinabyte.com/449/12385449.shtml>

2. Kindle Touch 出现远程代码执行漏洞

最近国外媒体报道 Kindle Touch 出现了远程可执行代码漏洞。针对 Kindle Touch 5.1.0 版本固件,可以远程执行代码,把/etc/shadow 文件发送到指定的 web 服务器。漏洞涉及到/usr/lib/libkindleplugin.so 插件,Kindle Touch 内置的浏览器 WebKit 会使用该插件。当用户浏览特定的网页时,就会以 root 权限执行特制的代码。当前 amazon 还没有相关补丁。可能会在下一个版本的固件升级中修复。

参考链接: <http://sec.chinabyte.com/380/12385380.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