

信息安全漏洞周报

2012年5月7日-2012年5月13日

2012年第19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 147 个，其中高危漏洞 69 个、中危漏洞 71 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 123 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“myCare2x CMS 存在多个 SQL 注入漏洞”、“iGuard Security Access Control 跨站脚本漏洞”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 147 个漏洞。各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰、安天实验室、天融信等单位报送数量较多。此外，奇虎公司、上海交通大学、北京邮电大学以及多位个人漏洞研究者向 CNVD 提交了 23 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	84	0
启明星辰	103	0
天融信	34	0
恒安嘉新	11	0
安天实验室	29	0
安氏领信	4	0
东软	5	0
奇虎	1	1
北京邮电大学	1	1

上海交通大学	13	13
个人报送者	8	8
报送总计	277	23
总计	147（去重）	23

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、Apple、Cisco、Adobe、Drupal 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	Microsoft	22	15.0%
2	Apple	15	10.2%
3	Cisco	15	10.2%
4	Adobe	13	8.8%
5	Drupal	8	5.4%
6	VMware	5	3.4%
7	EMC	3	2.0%
8	HP	3	2.0%
9	SAP	3	2.0%
10	IBM	1	0.7%
11	其它	59	40.3%

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 147 个漏洞。其中操作系统漏洞 23 个，应用程序漏洞 88 个，WEB 应用漏洞 27 个，安全产品漏洞 3 个，网络设备漏洞 6 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	23
应用程序漏洞	88
WEB 应用漏洞	27
网络设备漏洞	6
数据库漏洞	0
安全产品漏洞	3

表 3 漏洞按影响类型统计表

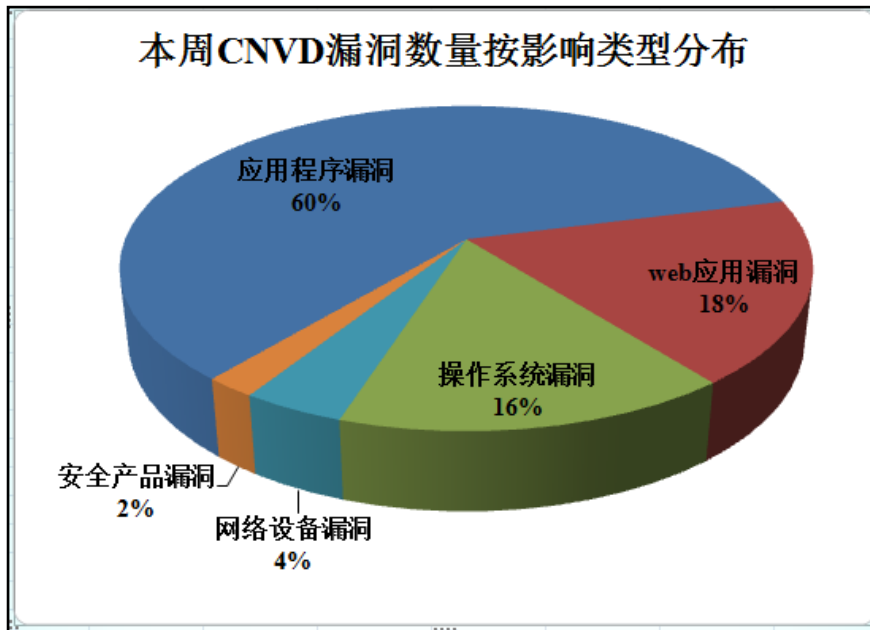


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 6 个网络设备漏洞，其中，“Cisco IOS NETIO 和 IPV4_IO 拒绝服务漏洞”、“Cisco IOS 'set mpls experimental imposition'命令拒绝服务漏洞”和“Cisco IOS Policy Feature Card 3C （PFC3C）拒绝服务漏洞”的综合评级为“高危”。“Symantec Web Gateway 'l'参数跨站脚本漏洞”和“Cisco Carrier Routing System 特殊 GRE 包分片报文拒绝服务漏洞”的综合评级为“中危”。“Cisco IOS 安全限制漏洞”的综合评级为“低危”。目前，互联网上已经出现针对“Symantec Web Gateway 'l'参数跨站脚本漏洞”的攻击代码。

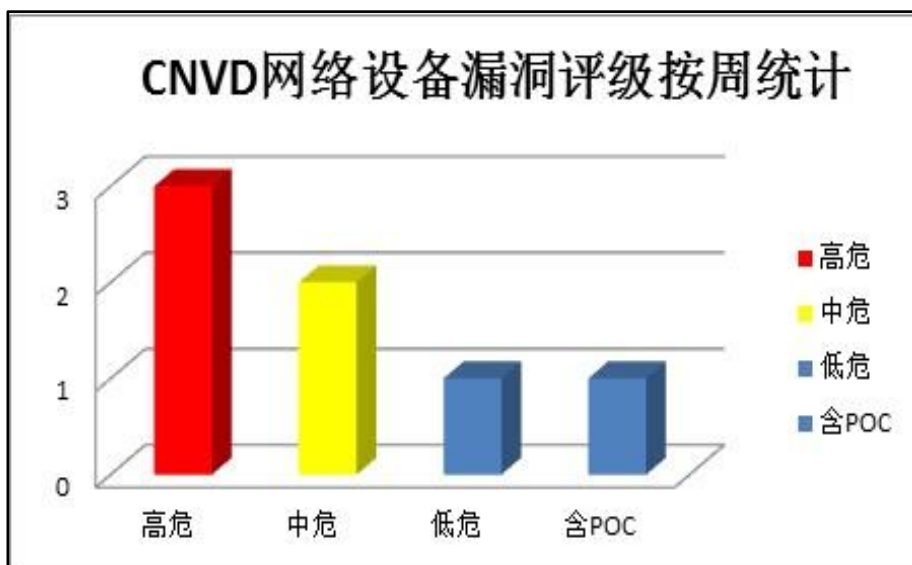


图 2 网络设备漏洞统计

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、Microsoft 产品安全漏洞

5 月 9 日，微软发布了 2012 年 5 月份的月度例行安全公告，共含 7 项更新，修复了 Microsoft Office、Windows、.NET Framework 和 Silverlight 中存在的 23 个漏洞。其中 3 项更新的综合评级为“严重”，其余 4 项均为“重要”。利用上述漏洞，攻击者可以远程执行代码，或本地提升特权。

CNVD 收录的相关漏洞包括：Microsoft Windows 本地特权提升漏洞（CNVD-2012-11763、CNVD-2012-11768）、Microsoft Excel 内存破坏远程代码执行漏洞（CNVD-2012-11747）、Microsoft Visio Viewer VSD File Format 远程代码执行漏洞（CNVD-2012-11780）、Microsoft Excel SXLI 记录内存破坏远程代码执行漏洞、Microsoft Excel 'MergeCells' 堆溢出远程代码执行漏洞（CNVD-2012-11749）、Microsoft .NET Framework 序列化远程代码执行漏洞（CNVD-2012-11739）、Microsoft Word RTF 数据处理远程内存破坏漏洞（CNVD-2012-11776）等。上述漏洞的综合评级均为“高危”。CNVD 提醒广大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=48623
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48607
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48640
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48611
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48609
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48599
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48628
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48636

2、Cisco 产品安全漏洞

Cisco IOS 是思科生产的网络操作系统；Cisco Carrier Routing System 是一款思科生产的路由系统；Cisco Adaptive Security Appliance 是一款自适应安全设备，可提供安全和 VPN 服务；Cisco Unified MeetingPlace 是一款思科统一通信产品中的多媒体协作解决方案；Cisco Prime LAN Management Solution 是一款局域网管理解决方案。本周，上述 Cisco 产品被披露存在多个安全漏洞，攻击者可以利用漏洞劫持用户会话、获得敏感信息或控制系统、发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Unified MeetingPlace SQL 注入漏洞、Cisco Unified MeetingPlace 跨站脚本漏洞、Cisco Prime LAN Management Solution HTTP 应答拆分漏洞、Cisco Unified MeetingPlace 目录枚举漏洞、Cisco IOS Policy Feature Card 3C

（PFC3C）拒绝服务漏洞、Cisco Adaptive Security Appliances (ASA) 5500 CRLF 注入漏洞、Cisco Carrier Routing System 特殊 GRE 包分片报文拒绝服务漏洞、Cisco IOS NETIO 和 IPV4_IO 拒绝服务漏洞等。

其中，“Cisco IOS NETIO 和 IPV4_IO 拒绝服务漏洞”、“Cisco Adaptive Security Appliances (ASA) 5500 CRLF 注入漏洞”、“Cisco IOS Policy Feature Card 3C （PFC3C）拒绝服务漏洞”的综合评级均为“高危”。目前，Cisco 已经发布这些漏洞的补丁，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=48690
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48687
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48692
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48686
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48577
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48544
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48535
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48554

3、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序；Adobe Photoshop 是一款图像处理软件；Adobe Flash Professional CS5.5 软件可以提供用于制作具有表现力的交互式内容的授权环境；Adobe Shockwave Player 是一款用于播放使用 Director Shockwave Studio 制作的网页的外挂软件；Adobe Illustrator 是一款矢量图编辑软件。本周，上述产品被披露存在多个安全漏洞，攻击者可以利用漏洞执行任意代码，远程控制受影响系统。

CNVD 收录的相关漏洞包括：Adobe Flash Player 对象类型混淆远程代码执行漏洞、Adobe Photoshop 缓冲区溢出漏洞、Adobe Flash Professional 缓冲区溢出漏洞、Adobe Shockwave Player 存在未明内存破坏漏洞（CNVD-2012-11754、CNVD-2012-11753、CNVD-2012-11756）、Adobe Illustrator 存在未明内存破坏漏洞（CNVD-2012-11738、CNVD-2012-11740）等。上述漏洞的综合评级均为“高危”。目前，厂商已经发布这些漏洞的修补程序，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=48485
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48608
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48596
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48614
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48598
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48613
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48600

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48616

4、Apple 产品安全漏洞

Apple Mac OS X 是一款苹果公司开发的操作系统；Apple Safari 是一款 WEB 浏览器。本周，上述产品被披露存在多个安全漏洞，攻击者可以利用漏洞构建恶意 WEB 页，诱使用户解析，发起钓鱼攻击、窃取敏感信息、拒绝服务攻击或执行任意代码。CNVD 收录的相关漏洞包括：Apple Mac OS X QuickTime 缓冲区溢出漏洞、Apple Mac OS X X.509 证书处理任意代码执行漏洞、Apple Mac OS X QuickTime MPEG 处理整数溢出漏洞、Apple Mac OS X QuickTime MPEG 处理缓冲区溢出漏洞、Apple Mac OS X 信息泄露漏洞、Apple Mac OS X QuickTime 内存错误引用漏洞、Apple Mac OS X 安全框架整数溢出漏洞、Apple Safari URI 欺骗漏洞等。其中，除“Apple Safari URI 欺骗漏洞”外，其余漏洞的综合评级均为“高危”。目前，厂商已经发布这些漏洞的修补程序，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=48751
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48746
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48735
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48736
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48747
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48737
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48739
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48553

5、myCare2x CMS 存在多个 SQL 注入漏洞

myCare2x 是一款 Web 应用程序。本周，myCare2x CMS 被披露存在一个综合评级为“高危”的 SQL 注入漏洞，主要影响 1.1 版本。攻击者可利用此漏洞在受影响的 dbms 中发起注入攻击，获得后台数据库信息或执行任意代码。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=48775

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-2012-11825	myCare2x CMS 存在多个 SQL 注入漏洞	高	暂无
CNVD-2012-11813	Galette 'picture.php' SQL 注入漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞进行 SQL 注入攻击，可操作数据库或控制

			应用系统: http://galette.tuxfamily.org/dc/index.php
CNVD-2012-11794	Lynx Message Server SQL 注入漏洞	高	暂无
CNVD-2012-11784	Serendipity SQL 注入漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞通过注入任意 SQL 代码操纵 SQL 查询： http://www.s9y.org/
CNVD-2012-11786	OrangeHRM SQL 注入漏洞 (CNVD-2012-11786)	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞获得数据库敏感信息： http://www.orangehrm.com/
CNVD-2012-11790	DecisionTools SharpGrid ActiveX 控件远程代码执行漏洞	高	暂无
CNVD-2012-11767	MyBB User Inline Moderation SQL 注入漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免允许攻击者进行恶意攻击： http://www.mybb.com/
CNVD-2012-11791	Core FTP LE 栈缓冲区溢出漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞以应用程序上下文执行任意代码： http://www.coreftp.com/
CNVD-2012-11707	MYRE Real Estate Mobile 存在多个 SQL 注入漏洞	高	暂无
CNVD-2012-11775	Netweaver DiagTraceR3Info 任意代码执行漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免允许远程未验证攻击者以运行"Dispatcher"服务特权执行任意代码： https://service.sap.com/sap/support/notes/1687910

表 3 部分高危漏洞列表

小结：5 月 9 日，微软发布了 2012 年 5 月份的月度例行安全公告，共含 7 项更新，修复了 Microsoft Office、Windows、.NET Framework 和 Silverlight 中存在的 23 个漏洞。其中 3 项更新的综合评级为“严重”，其余 4 项均为“重要”。利用上述漏洞，攻击者可以远程执行代码，或本地提升特权。

本周，Cisco、Adobe、Apple 的多款产品被披露存在多个漏洞，攻击者可以利用漏洞劫持用户会话、获得敏感信息或控制系统、发起拒绝服务攻击或执行任意代码。此外，myCare2x CMS 则被披露存在零日漏洞。

请使用相关产品的用户注意加强防范。

CNVD 整理和发布以下重要安全修补信息。

1、HP 发布升级程序，修补 Performance Insight 安全漏洞

本周，HP 发布升级程序，修补了 Performance Insight 存在的安全漏洞。攻击者可以利用漏洞进行未授权的访问、获得敏感信息控制应用系统或操作数据库。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=16812
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=16811

本周要闻速递

1. 微软 MAPP 数据泄露导致早期 RDP 漏洞利用

中国一家公司泄露了微软主动防护计划(Microsoft Active Protections Program, MAPP)中的漏洞数据，导致出现针对远程桌面协议(Remote Desktop Protocol, RDP)漏洞的早期漏洞利用。微软公司表示杭州某公司在修复补丁发布前泄露了漏洞信息，这违反了微软 MAPP 计划中的保密协议。微软在发出安全公告前，会向参与微软 MAPP 计划的安全供应商发送漏洞数据和修复信息，以给这些安全供应商足够的时间为其安全产品开发防护措施。微软对于泄密事件在微软安全响应中心的博客中写道：“微软非常重视对保密协议的遵守情况，并已将该公司从 MAPP 计划的名单中除名。”

参考链接：<http://security.ctocio.com.cn/143/12331643.shtml>

2. 苹果修复 Safari 漏洞 禁用老版 Flash Player

北京时间 5 月 10 日消息，苹果发布了针对 Safari 浏览器四个安全漏洞的补丁，同时阻止旧版本的 Adobe Flash Player 在这个浏览器上运行。苹果禁用旧版 Flash Player 之举与上个月推出的一项举措相似，当时苹果禁止 Java 插件自动运行。苹果发布了 Safari 5.1.7，可在 OS X 10.6 和 10.7（也就是雪豹和 Lion 操作系统）上运行，此外还能在 Windows XP、Vista 和 Windows 7 系统上运行。苹果同时还发布了另一个针对 Lion 系统的更新，这个系统含有稍老版本的 Safari 浏览器。Lion 用户必须下载和安装这两个更新，才能将其 Safari 浏览器升级到 5.1.7 版本。苹果周二为 iPhone、iPad 和 iPod Touch 发布了 iOS 5.1.1 升级补丁，对 iOS 平台的四个漏洞进行了修复，而 Safari 5.1.7 所修复的也正是这些漏洞。苹果对这些漏洞的描述都是 WebKit 上的漏洞，WebKit 是一个开源渲染引擎，为 Safari 和谷歌 Chrome 浏览器提供支持。除了修复这四个漏洞以外，苹果还禁止版本老于 10.1.102.64 的 Adobe Flash Player 在 Safari 浏览器上运行。10.1.102.64 版本是在 2010 年 11 月份发布的，自那以来 Adobe 开始为 Mac 配备 Flash Player 11。Adobe 同时还继续为 Flash Player 10 提供维护，目前其版本为 10.3.183.19。苹果顾问表示：“这个更新将把老于 10.1.102.64 版本的 Adobe Flash Player 文件移动到

新的目录下，从而禁用较老的版本。这个更新给出了一种选择，可让用户从 Adobe 网站安装新版本的 Flash Player。”

参考链接：<http://tech.qq.com/a/20120510/000323.htm>

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，支持基础信息网络安全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