

信息安全漏洞周报

2012 年 6 月 11 日-2012 年 6 月 17 日

2012 年第 24 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 104 个，其中高危漏洞 44 个、中危漏洞 58 个、低危漏洞 2 个。上述漏洞中，可利用来实施远程攻击的漏洞有 93 个。本周收录的漏洞中，已有 68 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“WordPress 插件 HTML5 AV Manager 'custom.php'任意文件上传漏洞”、“Gekko CMS 本地文件泄露漏洞”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报送了本周收录的全部 104 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、恒安嘉新、天融信、安天实验室等单位报送数量较多。此外，上海交通大学以及 3 位个人漏洞研究者向 CNVD 提交了 5 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	132	0
恒安嘉新	56	0
启明星辰	53	0
安天实验室	29	0
天融信	21	0
安氏领信	4	0
个人报送者	3	3
上海交通大学	2	2
报送总计	300	5

总计	104（去重）	5
----	---------	---

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、Wordpress、Adobe、Opera 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	25	24%
2	Wordpress	22	21%
3	Adobe	8	8%
4	Opera	5	5%
5	Gallery	3	3%
6	Ruby on Rails	2	2%
7	HP	1	1%
8	Cisco	1	1%
9	IBM	1	1%
10	Oracle	1	1%
11	其它	35	33%

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 104 个漏洞。其中操作系统漏洞 8 个，应用程序漏洞 44 个，WEB 应用漏洞 47 个，网络设备漏洞 2 个，数据库漏洞 2 个，安全产品漏洞 1 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	44
WEB 应用漏洞	47
网络设备漏洞	2
数据库漏洞	2
安全产品漏洞	1

表 3 漏洞按影响类型统计表

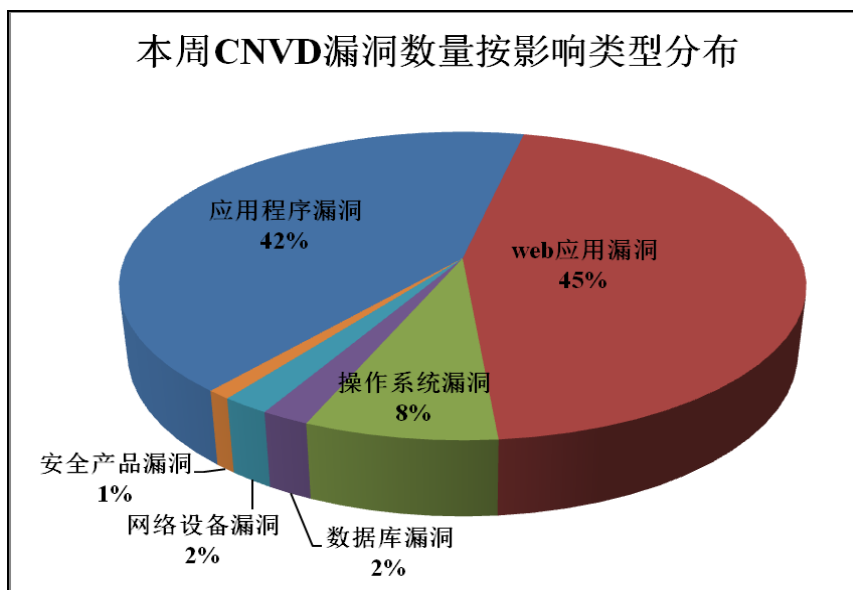


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 2 个网络设备漏洞，其中，“F5 BIG-IP 存在 root 用户权限验证绕过漏洞（CNVD-2012-12481）”的综合评级为“高危”，“Cisco Small Business 设备跨站脚本漏洞（CNVD-2012-12502）”的综合评级均为“中危”。目前，互联网上已经出现针对“F5 BIG-IP 存在 root 用户权限验证绕过漏洞”的攻击代码，CNVD 通过 CNCERT 通报平台向通信行业用户发布了预警通报。

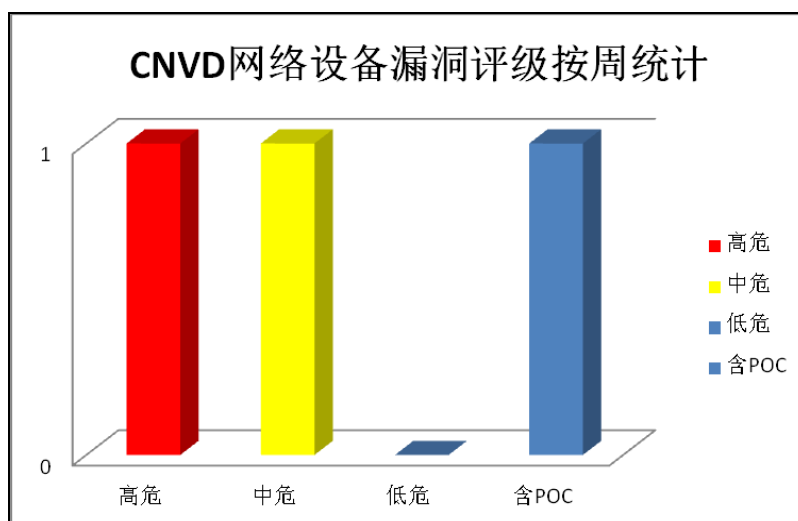


图 2 网络设备漏洞统计

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、F5 BIG-IP 存在 root 用户权限验证绕过漏洞

F5 BIG-IP 是由 F5 Network 公司生产的用于应用交付服务的设备产品，主要用于负载均衡、业务加速优化等用途。根据披露的情况，F5 BIG-IP（11.x/10.x/9.x 版本）设备文件系统中存在一组公开的 SSH 公私钥对，可用于用户权限验证，且验证通过后得到的是 root 用户权限。利用漏洞可以远程获取设备的管理控制权，进一步可发起针对相关网络信息系统的攻击。

CNVD 对该漏洞的综合评级为“高危”。根据 F5 BIG-IP 的应用情况，CNVD 评估认为该漏洞对我国基础电信运营企业以及相关互联网业务经营者构成较大威胁。目前，厂商已经发布安全公告。CNVD 建议广大企业和个人用户将产品升级至不受漏洞影响的版本。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50485

2、Microsoft 产品安全漏洞

Microsoft Internet Explorer 是一款 WEB 浏览器；Microsoft Windows 是微软研发的一款操作系统；Microsoft .NET Framework 是一套由微软分发的帮助开发者构建基于 WEB 应用的系统。本周，微软公司在 6 月的月度例行公告中发布了上述微软产品存在的多个漏洞补丁。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 'Title'元素更改远程代码执行漏洞、Microsoft Internet Explorer OnBeforeDeactivate 事件远程代码执行漏洞、Microsoft Internet Explorer insertAdjacentText 方法远程代码执行漏洞、Microsoft Windows 远程桌面协议对象处理漏洞、Microsoft .NET Framework WinForms 内存访问漏洞、Microsoft Internet Explorer toStaticHTML 过滤漏洞、Microsoft Internet Explorer 开发工具栏远程代码执行漏洞、Microsoft Internet Explorer EUC-JP 编码处理漏洞等，攻击者可以利用漏洞获取敏感信息或执行任意代码。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=50500

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50502

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50503

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50478

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50487

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50489

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50493

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50490

3、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，该产品被披露存在多个安全漏洞，攻击者可以利用漏洞绕过预设的访问限制，获得敏感信息，发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 访问限制绕过漏洞、Adobe Flash Player 栈溢出任意代码执行漏洞、Adobe Flash Player 内存破坏漏洞（CNVD-2012-12437）、Adobe Flash Player 空指针引用漏洞、Adobe Flash Player 内存破坏漏洞（CNVD-2012-12436）、Adobe Flash Player 不可信搜索路径漏洞、Adobe Flash Player 任意代码执行漏洞。其中，“Adobe Flash Player 不可信搜索路径漏洞”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=50357
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50359
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50361
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50362
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50360
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50358
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50363

4、Apple iTunes .m3u 播放列表处理堆溢出漏洞

Apple iTunes 是一款免费用于 Mac 和 PC 的应用程序。本周，该产品被披露存在一个播放列表处理堆溢出漏洞。攻击者可以构建恶意文件，诱使应用程序解析，可以应用程序上下文执行任意代码。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=50483

5、WordPress 插件 HTML5 AV Manager 'custom.php'任意文件上传漏洞

WordPress 是一款使用 PHP 语言开发的内容管理系统。本周，WordPress 插件 HTML5 AV Manager 'custom.php'被披露存在一个综合评级为“高危”的任意文件上传漏洞。攻击者可以利用漏洞在 web 服务器上传并执行任意 PHP 代码，可能导致未授权的访问或权限提升，从而执行其他攻击。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=50379

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-2012-12460	Agora Project 'dossierup'任意文件上传漏洞	高	暂无
CNVD-2012-12469	ClanSuite 任意文件上传漏洞	高	目前官方已对此漏洞发布相关补丁和临时处理方案，请及时关注网站最新动态： http://clansuite.com/
CNVD-2012-12454	WordPress Front File Manager 任意文件上传漏洞	高	暂无
CNVD-2012-12444	Best Practical Solutions RT 任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://lists.bestpractical.com/pipermail/rt-announce/2012-May/000204.html
CNVD-2012-12452	b2ePMS 存在多个 SQL 注入漏洞	高	暂无
CNVD-2012-12432	MyBB 'customfield'参数 SQL 注入漏洞	高	暂无
CNVD-2012-12518	Contao 'field' SQL 注入漏洞	高	Contao 2.11.4 版本已修复此漏洞建议用户下载使用： http://www.contao.org/
CNVD-2012-12531	Cells Blog CMS SQL 注入漏洞	高	暂无
CNVD-2012-12478	MariaDB/MySQL 身份认证登录漏洞	高	MariaDB 5.1.62, 5.2.12, 5.3.6, 5.5.23 和 MySQL 5.1.63, 5.5.24, 5.6.6 已经修复此漏洞，建议用户下载更新： http://www.mysql.com http://www.MariaDB.org
CNVD-2012-12513	Joomla! Art Uploader 模块任意文件上传漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，F5 BIG-IP 被披露存在一个 root 用户权限验证绕过漏洞，攻击者可以利用漏洞远程获取设备的管理控制权，进而可发起针对相关网络信息系统的攻击，对我国基础电信运营企业以及相关互联网业务经营者构成较大威胁。Microsoft、Apple 和 Adobe 产品存在的漏洞可被利用执行任意代码或获取敏感信息，由于这些产品用户较多，因此需引起企业和个人用户重视。此外，WordPress 插件 HTML5 AV Manager 'custom.php'被披露存在的零日漏洞，也对网络安全构成威胁，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、Oracle 发布升级程序，修补 Java Runtime Environment 组件安全漏洞

Java Runtime Environment 是一款为 JAVA 应用程序提供可靠的运行环境的解决方案。本周，Oracle 发布升级程序，修补了 Java Runtime Environment 组件存在的漏洞。攻击者可以利用漏洞执行任意代码。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=18096

本周要闻速递

1. comex 加入苹果或是 iOS6 封堵重要漏洞的原因

iOS6 发布后，虽然 iPhone-Dev Team 团队迅速发布了一个针对开发版本的 0.9.13 dev1，来针对 iOS6 实现越狱，不过遗憾的是无法实现安装 Cydia。而越狱黑客的另一重量级人物 Pod2g，更是透露了一则不算好的消息，苹果已经在 iOS6 中封堵了一个已经存在两年的重要漏洞。该漏洞由前越狱黑客 comex 发现，comex 以研发 JailbreakMe1.0 和 2.0 版本，成功越狱 iOS3 和 iOS4.3.3，同时也是首次实现 iPad2 完美越狱的方法。

参考链接：<http://iphone.tgbus.com/news/class/201206/20120617091843.shtml>

2. CPU 漏洞导致 64 位操作系统易受黑客攻击

美国计算机应急预备小组本周发布了一份安全报告，一些 64 位操作系统和虚拟化软件程序在 Intel 处理器上运行时，容易受到本地特权扩大攻击(local privilege escalation)。该漏洞可能被利用来获取本地特权扩大或是 guest-to-host 虚拟机逃逸(virtual machine escape)。这一漏洞(CVE-2012-0217)源于 Intel 处理器在 x86-64 扩展(也就是 Intel 64)中执行 SYSRET 指令集的方式，仅仅影响 Intel 处理器上的 Intel 64 扩展使用，32 位操作系统或虚拟化软件不受影响。受影响的操作系统包括：64 位 Windows 7、Windows Server 2008 R2、64 位 FreeBSD 和 NetBSD、Xen 虚拟化软件、红帽企业 Linux、SUSE Linux Enterprise Server。VMware 安全团队表示，VMware 的管理程序不使用 SYSRET 指令集，因此，VMWare 不受此漏洞影响。

参考链接：<http://tech.sina.com.cn/s/2012-06-16/11097276471.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