

信息安全漏洞周报

2011 年 4 月 4 日-2011 年 4 月 10 日

2011 年第 14 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**低**。

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 54 个,其中高危漏洞 12 个、中危漏洞 24 个、低危漏洞 18 个。上述漏洞中,可利用来实施远程攻击的漏洞有 46 个。网上已经出现针对“Graugon Forum SQL 注入漏洞”和“Banner Ad Management Script SQL 注入漏洞”等的零日攻击代码,请使用相关产品的用户注意做好防护措施。本周收录的漏洞中,已有 31 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。

成员单位上报漏洞统计

本周,共有 5 家成员单位报送了本周收录的全部 54 个漏洞,各单位报送情况如表 1 所示。其中,启明星辰、恒安嘉新报送数量较多。

成员单位	漏洞上报总数	私有漏洞数量
启明星辰	39	0
绿盟科技	9	0
安氏领信	1	0
东软	5	0
恒安嘉新	18	0
总计	54 (去重)	0

表 1 成员单位上报漏洞统计表

本周, CNVD 整理和发布了 Mono、FFmpeg、WordPress、Microsoft 等多家厂商(产品)的漏洞,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	Mono	4	7.4%
2	Logrotate	4	7.4%
3	FFmpeg	3	5.6%
4	Rsyslog	3	5.6%
5	RealNetworks	2	3.7%
6	WordPress	2	3.7%
7	Apache	2	3.7%
8	Microsoft	1	1.9%
9	Linux	1	1.9%
10	其他	32	59.1%

表 2 漏洞产品涉及厂商分类统计

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 Vista TCP/IP 堆缓冲区下溢漏洞

Microsoft Vista 是一款微软开发的操作系统。本周，Microsoft Vista 被披露存在一个综合评级为“高危”的安全漏洞。Windows Vista 32 位和 64 位系统发布的 API 中封装的 Microsoft Device IO Control 存在一个缓冲区溢出漏洞，远程攻击者可利用此漏洞使操作系统崩溃。目前，微软尚未发布该漏洞的补丁程序，CNVD 建议用户及时关注厂商主页，以获取补丁程序或最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04952>

2、logrotate 产品安全漏洞

logrotate 是一款日志文件管理工具。本周，logrotate 出现了本地攻击漏洞。本地攻击者可以利用漏洞执行任意 SHELL 命令、提升特权、窃取敏感信息或进行其他未授权操作。CNVD 收录的 logrotate 漏洞包括：logrotate 'shred_file()' 日志文件名命令注入漏洞、logrotate Debian Linux 'var/log/postgresql' 符号链接本地特权提升漏洞、logrotate Gentoo Linux 'var/log/' 符号链接本地特权提升漏洞、logrotate 'writeState()' 函数日志文件名本地拒绝服务漏洞、logrotate 默认文件权限信息泄露漏洞。除“logrotate Debian Linux 'var/log/postgresql' 符号链接本地特权提升漏洞”和“logrotate Gentoo Linux 'var/log/' 符号链接本地特权提升漏洞”外，厂商已经发布其余漏洞的补丁程序，CNVD 提醒相关用户及时获取补丁程序进行修补。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04918>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04917>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04916>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04915>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04877>

3、Moonlight 产品安全漏洞

本周，Moonlight 产品被披露存在多个安全漏洞。Moonlight 是 Microsoft Silverlight 对应的 Linux 开源版本。CNVD 收录的相关漏洞包括：Moonlight 2.4.1/3.99.3 之前版本存在安全漏洞（CVE-2011-0992、CVE-2011-0991、CVE-2011-0990、CVE-2011-0989）。攻击者可以利用这些漏洞绕过安全限制，执行未授权操作或者获得敏感信息。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了这些漏洞的补丁程序，CNVD 提醒相关用户及时获取补丁程序进行修补。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04936>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04935>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04934>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04933>

4、Apache Tomcat 安全漏洞

Apache Tomcat 是一款开放源码的 JSP 应用服务器程序。本周，Apache Tomcat 出现了两个安全漏洞。CNVD 收录的相关漏洞包括：Apache Tomcat HTTP BIO 连接器信息泄露漏洞、Apache Tomcat 登录 Constraints 安全绕过漏洞。攻击者可以利用漏洞绕过验证、获得敏感信息。目前，Apache 已经发布了补丁程序，CNVD 提醒广大用户及时下载修复。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04931>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04930>

5、Graugon Forum 和 Banner Ad Management Script WEB 应用漏洞

本周，Graugon Forum 和 Banner Ad Management Script 产品均被披露存在综合评级为“高危”的安全漏洞。Graugon Forum 是一款使用 php 编写的 BBS 系统；Banner Ad Management Script 是一款网站横幅广告管理系统。上述两个产品均存在 SQL 注入漏洞，攻击者可以利用漏洞窃取敏感信息。CNVD 收录的漏洞包括：Graugon Forum SQL 注入漏洞、Banner Ad Management Script SQL 注入漏洞。目前，互联网上已经出现针对这两个漏洞的攻击代码，且厂商尚未发布这两个漏洞的补丁，CNVD 建议用户及时关注厂商主页，以获取补丁程序或最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04929>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04942>

小结：本周，Microsoft Vista 被披露存在一个缓冲区溢出漏洞，攻击者可利用此漏洞使系统崩溃，对 Vista 用户构成较大威胁。logrotate、Moonlight 和 Apache Tomcat 等应用较为广泛的软件产品均被披露了安全漏洞。此外，Graugon Forum 和 Banner Ad Management Script

两款 WEB 应用产品也出现了多个安全漏洞，对使用上述产品的网站构成较大威胁。请使用上述软件的相关机构和个人及时采取安全防范措施。

本周重要漏洞修补信息

本周，CNVD 整理和发布以下重要安全修补信息。

1、FFmpeg 发布升级程序，修补多个安全漏洞

本周，FFmpeg 发布升级程序，修补了该产品多个安全漏洞。攻击者利用漏洞可造成应用程序崩溃或以应用程序权限在用户上下文中执行任意代码。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/patch/3439>
<http://www.cnvd.org.cn/patch/3440>
<http://www.cnvd.org.cn/patch/3441>

本周要闻速递

1. 微软本月将发布 17 个安全公告 修复 64 个漏洞

微软将在美国东部时间 4 月 12 日星期二下午 1 点发布将公布 17 个安全公告，修复 64 个漏洞，产品涉及 Microsoft Windows, Microsoft Office, Internet Explorer, Visual Studio, .NET Framework 和 GDI+。其中 9 个安全公告的评级为“严重”，其余均为“重要”。这些补丁包括一个 IE 浏览器的更新，用于修复两个已经公开的安全漏洞。微软称，本月将修复微软已经披露的一些安全漏洞，包括在 2 月 15 日公开披露的 SMB 浏览器漏洞（评级为“严重”）。微软对 SMB 浏览器漏洞进行了评估，认为：尽管这个安全漏洞在理论上允许远程执行代码，但是在实际上是不可能；而且到目前为止，还没有看到任何攻击的证据。微软还计划修复 Windows 中的 HTML 安全漏洞，这个安全漏洞的评级是“重要”。微软没有说这次 IE 更新是否要修复在 CanSecWest Pwn2Own 黑客大会中获奖的攻击中利用的多个 IE 漏洞。微软这次发布的补丁涉及所有版本的 Windows 操作系统，包括最新的 Windows 7。

参考链接：<http://www.7747.net/News/201104/87193.html>

2. 俄罗斯总统博客遭黑客攻击

国际文传电讯社报道，梅德韦杰夫在知名博客网站 LiveJournal 开设的博客 6 日遭遇“分布式拒绝服务”攻击，至少 1 小时无法访问。梅德韦杰夫 7 日在博客上写道，“作为一名活跃博主，我认为这种行径非法且不可容忍”，网站管理者和执法机构应着手调查。声明发表半小时后，大约 20 名网友跟贴留言，声援梅德韦杰夫。不少博主希望俄罗斯政府出台相关措施遏制网络黑客攻击。

参考链接：<http://www.7747.net/News/201104/87289.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