

信息安全漏洞周报

2011 年 5 月 2 日-2011 年 5 月 8 日

2011 年第 18 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 80 个，其中高危漏洞 37 个、中危漏洞 38 个、低危漏洞 5 个。上述漏洞中，可利用来实施远程攻击的漏洞有 69 个。网上已经出现针对“BMC Remedy Knowledge Management 跨站脚本漏洞”、“SPlayer 'Content-Type'头远程缓冲区溢出漏洞”等的零日攻击代码，请使用相关产品的用户注意做好防护措施。本周收录的漏洞中，已有 56 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 6 家成员单位和 1 位个人上报者报送了本周收录的全部 80 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、绿盟科技报送的数量较多。国外安全研究者 Dillon Beresford 向 CNVD 报送涉及国内邮件系统软件生产厂商、嵌入式系统平台 VxWorks 的两个漏洞，将在完成处置流程后择时发布漏洞公告。此外，知道创宇报送了 3 个网站安全漏洞，包括：人民网注入漏洞、华北科技学院网站上传漏洞、交通银行网站目录遍历漏洞。上述漏洞事件转由国家互联网应急中心（CNCERT）纳入安全事件处置流程，未分配 CNVD 漏洞编号。

成员单位	漏洞上报总数	私有漏洞数量
启明星辰	67	0
绿盟科技	6	0
恒安嘉新	11	0
东软	1	0
安氏领信	1	0
知道创宇	3	0
个人上报者	2	0
总计	80（去重）	0

表 1 成员单位上报漏洞统计表

本周，CNVD 整理和发布的漏洞涉及 Ubuntu、Mozilla、HP、Linux、BMC、VideoLAN 等多家厂商的产品，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	Ubuntu	17	21.3%
2	Mozilla	15	18.8%
3	HP	10	12.5%
4	Proofpoint	5	6.3%
5	Linux	2	2.5%
6	BMC	4	5.0%
7	Red Hat	2	2.5%
8	ICONICS	1	1.3%
9	VideoLAN	1	1.3%
10	其他	23	28.5%

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、Mozilla 发布安全公告，修复多个产品安全漏洞

本周，Mozilla 发布了公告，修复 Seamonkey、Firefox、Thunderbird 产品的多个安全漏洞。攻击者可以利用这些漏洞获取敏感信息、破坏内存或执行任意代码。CNVD 收录的 Mozilla 漏洞包括：Mozilla Firefox/Thunderbird/SeaMonkey HTML 内容内存破坏漏洞（CVE-2011-0081、CVE-2011-0080）、Mozilla Firefox/SeaMonkey 内存破坏漏洞（CVE-2011-0072、CVE-2011-0073、CVE-2011-0066）、Mozilla Firefox/SeaMonkey 两次释放内存破坏漏洞、Mozilla Firefox/SeaMonkey Marquee 元素内存破坏漏洞、Mozilla Firefox/Thunderbird/SeaMonkey 跨域 JavaScript 内存破坏漏洞、Mozilla Firefox/Thunderbird/SeaMonkey HTML Iframe 标签内存破坏漏洞、Mozilla Firefox/Thunderbird/SeaMonkey 内存破坏漏洞（CVE-2011-0078、CVE-2011-0065、CVE-2011-0079）、Mozilla Firefox/SeaMonkey 特权提升漏洞（CVE-2011-0076）、Mozilla Firefox/Thunderbird/SeaMonkey 'resource:'协议目录遍历漏洞、Mozilla Firefox/SeaMonkey 信息泄露漏洞（CVE-2011-0067）。除“Mozilla Firefox/Thunderbird/SeaMonkey HTML 内容内存破坏漏洞（CVE-2011-0080）”外，其余漏洞的综合评级为“高危”。CNVD 提醒广大 Mozilla 用户及时下载补丁程序进行修补。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05321>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05317>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05316>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05315>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05314>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05313>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05305>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05312>

2、HP 产品安全漏洞

HP OpenView Storage Data Protector 是一款实现基于磁盘或磁带的高性能备份和恢复的解决方案。HP Insight Control 是 HP 发行的一款综合系统管理解决方案。本周上述产品出现了多个安全漏洞。远程攻击者可以利用漏洞查看或下载目标系统文件、提升特权或执行任意代码。CNVD 收录的相关漏洞包括：HP OpenView Storage Data Protector 远程代码执行漏洞（CVE-2011-1736）、HP Insight Control for Linux (CVE-2011-1535)未明特权提升漏洞、HP OpenView Storage Data Protector 远程代码执行漏洞（CVE-2011-1735、CVE-2011-1734、CVE-2011-1733、CVE-2011-1732、CVE-2011-1731、CVE-2011-1730、CVE-2011-1729、CVE-2011-1728）。除“HP Insight Control for Linux (CVE-2011-1535)未明特权提升漏洞”外，其余漏洞的综合评级均为“高危”，且厂商已经发布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-2011-05335>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05334>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05333>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05330>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05328>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05327>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05326>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05325>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05324>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05323>

3、BMC 产品安全漏洞

BMC Remedy 知识库管理是一个用于创建、出版、审查和搜索 IT 资讯知识文章的解决方案。BMC Dashboards 是一款用于 BSM 决策支持自动化的运营管理分析软件。本周上述产品存在多个安全漏洞。攻击者可以利用漏洞发起跨站脚本攻击，获取敏感信息或绕过安全限制。CNVD 收录的漏洞包括：BMC Remedy Knowledge Management 跨站脚本漏洞、BMC Remedy Knowledge Management 默认账户漏洞、BMC Dashboards 信息泄露漏洞、BMC Dashboards 跨站脚本漏洞。互联网上已经出现该漏洞的攻击代码，主要影响 BMC Dashboards 7.6.0 和 Remedy Knowledge Management 7.5.00 版本。厂商尚未发布漏洞的补丁程序，CNVD 提醒广大用户随时关注厂商主页获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05345>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05344>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05343>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05342>

4、SPlayer 'Content-Type' 头远程缓冲区溢出漏洞

SPlayer 是一款媒体播放程序。当解析远程服务器返回的特制的 HTTP 头字段时存在缓冲区溢出漏洞。攻击者通过诱使用户打开特制的播放列表文件，用其中包含的 URL 指向恶意 WEB 服务器来触发漏洞。目前，互联网上已经出现该漏洞的攻击代码，主要影响 Splay er 3.7 版本。厂商尚未发布漏洞的补丁程序，CNVD 提醒广大用户随时关注厂商主页获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05329>

5、ICONICS VersionInfo ActiveX 控件缓冲区溢出漏洞

GENESIS32/64 是由美国 ICONICS 公司研制开发的新一代工控软件。ICONICS Versio nInfo ActiveX 控件存在安全漏洞，"SetActiveXGUID()"方法(GenVersion.dll)存在边界错误，向"Ax_GUID"参数传递超长字符串，可触发基于栈的缓冲区溢出。允许攻击者构建恶意 W EB 页，诱使用户解析，以应用程序上下文执行任意代码。目前，互联网上已经出现该漏洞的攻击代码，主要影响 ICONICS VersionInfo ActiveX Control、GENESIS64、GENESIS32、BizViz 多个产品。目前，厂商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-2011-05338>

小结：本周，Mozilla 发布安全公告，修复了 Seamonkey、Firefox、Thunderbird 产品的多个综合评级为“高危”的安全漏洞。攻击者可以利用这些漏洞获取敏感信息、破坏内存或执行任意代码，对广大 Mozilla 用户构成较为严重的威胁。HP、BMC 和 ICONICS 产品均出现了安全漏洞，且部分漏洞的攻击代码已在互联网上出现。此外，SPlayer 和 BMC 产品出现了零日漏洞，对使用该产品的用户构成较大威胁。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、Proofpoint 发布升级程序，修补 Proofpoint Protection Server 多个安全漏洞

本周，Proofpoint 发布升级程序，修补了 Proofpoint Protection Server 存在的多个安全漏洞。Proofpoint Protection Server 是一款电子邮件安全服务解决方案。攻击者利用漏洞可以获取敏感信息或提升特权。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/3746>

<http://www.cnvd.org.cn/patch/3747>

<http://www.cnvd.org.cn/patch/3748>

<http://www.cnvd.org.cn/patch/3749>

<http://www.cnvd.org.cn/patch/3750>



本周要闻速递

1. 微软下周将修复三个安全漏洞

5月6日消息，微软将在5月10日补丁星期二发布两个补丁，修复 Windows 服务器软件中的一个严重安全漏洞和 PowerPoint 软件中的两个安全漏洞。在微软发布的两个补丁中，一个补丁的等级是“严重”，是微软四个威胁级别中最严重的。另一个补丁的等级是“重要”，是排在第二位的威胁等级。这个严重等级的补丁修复 Windows 服务器软件中的安全漏洞，如 Windows Server 2003、Windows Server 2008 和 Windows Server 2008 R2，以及三个仍提供技术支持版本的微软服务器操作系统。微软称，另一个安全补丁适用于 Office XP、Office 2003 和 Office 2007。微软特别指出 PowerPoint 是使用这个补丁的 Office 程序。微软还将发布补丁修复 Office 2004 for Mac 和 Office 2008 for Mac 软件中的安全漏洞。下周发布的用于 Office XP 版 PowerPoint 的补丁将是得到的最后的补丁之一。这个已经有 10 年时间的套装软件在 7 月 12 日之后将得不到安全更新。最新版本的 Windows 平台的 Office 2010 和 Office 2011 for Mac 不受这个 PowerPoint 安全漏洞的影响。

参考链接：http://news.ccidnet.com/art/11099/20110506/2381665_1.html

2. Mac 版 Skype 客户端软件出现零日漏洞，可被黑客利用

据国外媒体报道，近日发现的一个 Mac 版 Skype 客户端软件的零日攻击漏洞可以使黑客通过发送即时信息来控制用户的系统。据悉，Skype 的这个漏洞非常危险，可以使得任何懂得如何控制 Mac 的人简单地通过发送恶意即时信息达成目的。Pure Hacking 公司的戈登-马登（Gordon Maddern）在其博客中称，他是在通过 Skype 向朋友发送客户负载时发现这一漏洞的。随后，他通过制作一个利用这个恶意负载的概念证明然后在 Skype 进行测试从而验证了自己的猜测。他在博客中写道：“黑客只需要向受害者发送一条信息即可远程控制 Mac，这就像蠕虫病毒般非常危险。”一个月之前马登就已经向 Skype 的安全小组报告了这一漏洞。而公司只给了一份非常唐突的回答，告知马登公司已知晓这一情况，将会尽快发布补丁。一个月之后，马登决定向公众公布这一漏洞，虽然他仍然会在补丁发布之前保留了一些关键细节。在马登公布信息的几小时之后，Skype 立即发布了补丁，称补丁能完全修复漏洞。

参考链接：<http://www.hackbase.com/news/2011-05-10/71196.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