

信息安全漏洞周报

2011 年 5 月 16 日-2011 年 5 月 22 日

2011年第20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 78 个，其中高危漏洞 27 个、中危漏洞 45 个、低危漏洞 6 个。上述漏洞中，可利用来实施远程攻击的漏洞有 70 个。网上已经出现针对“Microsoft Windows 'nsiproxy.sys'驱动本地拒绝服务漏洞”、“Wordpress is_human()插件远程命令注入漏洞”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 38 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。

成员单位报送漏洞统计

本周，共有 6 家成员单位报送了本周收录的全部 78 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。此外，安天报送了 5 个政府网站 SQL 注入漏洞，涉及中国气象局气候研究开放实验室、中德科技合作长春网络平台、广东惠东县质量技术监督局、营口市西市区政务信息网、中国节能监察信息网山西省分站。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。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	66	0
绿盟科技	11	0
恒安嘉新	27	0
东软	5	0
安氏领信	1	0
安天	6	0
总计	78（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 IBM、Linux、Microsoft、Cisco、Red Hat 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	IBM	5	6.3%
2	Linux	5	6.3%
3	Cisco	4	5.1%
4	Apache	3	3.8%
5	Xtreamer LTD.	3	3.8%
6	Red Hat	2	2.5%
7	TIBCO	2	2.5%
8	WordPress	2	2.5%
9	Microsoft	1	1.3%
10	其他	52	65.9%

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、勤云科技远程稿件处理系统文件上传漏洞

勤云科技公司生产的远程稿件处理系统由于未能对上传文件格式或文件上传目录读写权限进行检查，致使攻击者可上传特定构造的网站后门文件，直接获得网站的管理权限。目前勤云科技公司未能提供漏洞补丁，建议采用以下临时措施：(1)强化网站投稿模块对文件上传类型的服务器端验证；(2)取消图片及稿件存储目录的执行权限；(3)建议将服务器组件由 IIS 6 升级至 IIS 7。该漏洞的综合评级为“高危”。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05428>

2、三维力控产品安全漏洞

本周，三维力控公司生产的两款工业控制系统软件 pNetPower 和 ForceControl 存在的缓冲区溢出漏洞。攻击者可以利用漏洞可发起远程攻击，导致工业控制系统崩溃，甚至可取得控制系统主机管理权限。CNVD 收录的漏洞包括：ForceControl 6.1 WebServer URI 请求堆缓冲区溢出漏洞、pNetPower 6.1 AngelServer UDP 数据包堆缓冲区溢出漏洞。上述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-2011-05348>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05347>

3、IBM 产品安全漏洞

本周，IBM 的 Virtualization Manager、Informix Dynamic Server 和 Datacap Taskmaster Capture 等多款产品存在安全漏洞。攻击者可以利用漏洞注入任意 SQL 代码，获取敏感信息或操作数据库。CNVD 收录的相关漏洞包括：IBM Datacap Taskmaster Capture 验证绕过漏洞、IBM Datacap Taskmaster Capture eDocument 转换操作拒绝服务漏洞、IBM Virtualization Manager 存在未明漏洞、IBM Informix 'librpc.dll'伪造漏洞、IBM DatacapTaskmaster Capture 未明 SQL 注入漏洞。其中，“IBM Informix 'librpc.dll'伪造漏洞、IBM DatacapTaskmaster Capture 未明 SQL 注入漏洞”的综合评级为“高危”。除“IBM DatacapTaskmaster Capture eDocument 转换操作拒绝服务漏洞、IBM Virtualization Manager 存在未明漏洞”外，IBM 已经发布其余漏洞的修补程序，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/vulnerability/CNVD-2011-05520>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05518>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05511>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05479>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05469>

4、Linux Kernel 安全漏洞

Linux 是一款开源操作系统。本周，Linux Kernel 出现多个安全漏洞，攻击者可以利用漏洞发起拒绝服务攻击或提升特权。CNVD 收录的相关漏洞包括：Linux Kernel 'ip_expire()'拒绝服务漏洞、Linux Kernel 隧道初始化远程拒绝服务漏洞、Linux Kernel 'IP GRE'模块空指针引用远程拒绝服务漏洞、Linux Kernel 'icmp_send()'空指针引用远程拒绝服务漏洞、Linux Kernel 'agp_ioctl()'本地特权提升漏洞。其中，“Linux Kernel 隧道初始化远程拒绝服务漏洞、Linux Kernel 'IP GRE'模块空指针引用远程拒绝服务漏洞、Linux Kernel'icmp_send()'空指针引用远程拒绝服务漏洞”的综合评级均为“高危”。除“Linux Kernel 'icmp_send()'空指针引用远程拒绝服务漏洞”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-2011-05529>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05483>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05482>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05481>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05471>

5、Cisco 产品安全漏洞

CiscoWorks Common Services 是 CiscoWorks 应用所共享的通用管理服务集。Cisco Unified Operations Manager 是思科统一通信管理套件的组成部分。本周，Cisco 上述两款产品

出现安全漏洞，远程攻击者可以利用漏洞获取敏感信息或劫持用户会话。CNVD 收录的相关漏洞包括：CiscoWorks Common Services 审计目录遍历漏洞、Cisco Unified Operations Managerc SQL 注入漏洞、Cisco Unified Operations Manager 跨站脚本漏洞、Cisco Unified Operations Manager Common Services 设备中心跨站脚本漏洞。其中，“Cisco Unified Operations Managerc SQL 注入漏洞”的综合评级为“高危”。除“CiscoWorks Common Services 审计目录遍历漏洞”外，厂商已经发布其余漏洞的补丁程序，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/vulnerability/CNVD-2011-05515>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05512>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05510>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05509>

6、Microsoft Windows 'nsiproxy.sys'驱动本地拒绝服务漏洞

Microsoft Windows 是一款流行的操作系统。Microsoft Windows Vista/Server 2008 "nsiproxy.sys"未能正确处理 IOCTL，攻击者可以利用此漏洞使内核崩溃，造成拒绝服务攻击。目前，互联网上已经出现该漏洞的攻击代码，主要影响 Windows Vista 和 Server 2008 多个版本。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-2011-05517>

7、WordPress 产品安全漏洞

WordPress 是一款流行的 blog 系统。本周，WordPress 出现了一个命令注入漏洞和一个文件上传漏洞。远程攻击者可以利用漏洞在受影响的程序中执行任意代码或获取 webshell。CNVD 收录的相关漏洞包括：WordPress EditorMonkey 'FCKeditor'远程文件上传漏洞、WordPress is_human()插件远程命令注入漏洞。目前，互联网上已经出现该漏洞的攻击代码，主要影响 Wordpress is_human()插件 1.4.2 版本和 WordPress EditorMonkey 插件 2.5 及之前版本。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-2011-05491>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05475>

小结：本周，CNVD 发布了“勤云科技远程稿件处理系统文件上传漏洞、三维力控组态软件缓冲区漏洞”多个综合评级为“高危”的漏洞，并发布了相应的补丁或临时修补措施，提醒使用上述产品的用户及时下载补丁更新进行修补。同时，CNVD 还收录了 IBM、Cisco、Linux 多个产品出现的安全漏洞以及 Microsoft Windows Vista/Server 2008 和 Wordpress 插件的多个零日漏洞，攻击者可以利用漏洞发起包括拒绝服务或远程执行任意代码等恶意攻击，对使用这些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、Apache 发布升级程序，修补多个产品安全漏洞

本周，Apache 发布升级程序，修补了 Apache Portable Runtime、Tomcat、Struts 多个产品存在的安全漏洞。远程攻击者可以利用漏洞发起拒绝服务攻击、获取敏感信息或执行任意代码。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/3886>

<http://www.cnvd.org.cn/patch/3885>

<http://www.cnvd.org.cn/patch/3921>

本周要闻速递

1. 索尼旗下网站再现安全漏洞

5 月 19 日消息，据悉，索尼又发现旗下网站存在安全漏洞，为保证用户利益，索尼昨日宣布暂时关闭存在数据泄漏风险的网页。据悉，索尼 PlayStation 网络、Qriocity 音乐服务和索尼在线娱乐的游戏服务不久前遭到黑客攻击，全球受影响的用户数量超过 1 亿，他们的家庭住址、电子邮件、生日、用户名和登录密码等信息，甚至包括信用卡的详细信息已被黑客窃取。索尼 CEO Howard Stringer 日前表示，索尼 PlayStation 网络被入侵事件将来可能引发更大的问题，不仅仅局限在索尼或整个游戏行业，黑客将来还可能将目标瞄向金融系统，电网或交通控制系统等等。他表示，PlayStation 网络已经在美国和欧洲部分恢复，并强化了安全措施。Stringer 称维护这些服务的安全“是一个没有尽头的过程”，没人可以确保这些服务“100%安全”。

参考链接：<http://games.sina.com.cn/y/n/2011-05-19/1127499208.shtml>

2. Android 存在安全漏洞 用户应避面使用公共 WiFi 网络

5 月 19 日消息，据国外媒体报道，研究报告警告，Android 智能手机用户最好避开使用公共 WiFi 网络，因为潜在的安全漏洞可能泄露使用者个人信息。德国乌尔姆大学 3 位研究员发现，黑客可以“相当容易”地截取谷歌照片分享，行动日历和联络人等应用程序中的数据，还有其他谷歌的服务（例如 Gmail 等），通过这安全漏洞，99% 的 Android 设备的用户都会受到影响。此报告披露的消息将再次让市场聚焦谷歌对手机操作系统的安全。此安全漏洞在 Android 2.3.4 版与之后的版本均已部分修正。谷歌表示：“我们意识到此问题了，也已经在 Android 的最新版本中修正了行动日历和联络人的问题，目前我们在修正的 Picasa

中的问题。”

参考链接: http://news.ccidnet.com/art/949/20110519/2394453_1.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