

信息安全漏洞周报

2011 年 4 月 25 日-2011 年 5 月 1 日

2011 年第 17 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 101 个，其中高危漏洞 34 个、中危漏洞 64 个、低危漏洞 3 个。上述漏洞中，可利用来实施远程攻击的漏洞有 95 个。网上已经出现针对“PHP 'phar/tar.c'堆缓冲区溢出漏洞”、“Netop Remote Control 'dws'文件缓冲区溢出漏洞”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 75 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 家成员单位报送了本周收录的全部 101 个漏洞，各单位报送情况如表 1 所示。其中，启明星辰报送数量较多。

成员单位	漏洞上报总数	私有漏洞数量
启明星辰	77	0
绿盟科技	7	0
安氏领信	2	0
东软	3	0
安天	1	0
恒安嘉新	24	0
总计	101（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 Google、Cisco、HP、Microsoft、Linux、IBM 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	Google	39	38.6%
2	Cisco	8	7.9%
3	Advantech	4	4.0%
4	HP	3	3.0%
5	Microsoft	3	3.0%
6	VMWare	2	2.0%
7	Linux	2	2.0%
8	IBM	1	1.0%
9	Mozilla	1	1.0%
10	其他	38	37.5%

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、Google Chrome 安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，Google Chrome 被披露存在多个安全漏洞，攻击者可以利用漏洞发起拒绝服务攻击，绕过同源策略，执行任意代码，获取敏感信息。CNVD 收录的相关漏洞包括：Google Chrome 11.0.696.57 之前版本存在安全漏洞（CVE-2011-1456、CVE-2011-1455、CVE-2011-1454）、Google Chrome 8.0.552.215 之前版本双重释放漏洞（CVE-2010-4494）、Google Chrome 8.0.552.215 之前版本拒绝服务漏洞（CVE-2010-4491、CVE-2010-4490）、Google Chrome 8.0.552.215 之前版本不完整黑名单漏洞（CVE-2010-4487）、Google Chrome 8.0.552.215 之前版本信息泄露漏洞（CVE-2010-4483）等。上述漏洞中，“Google Chrome 11.0.696.57 之前版本存在安全漏洞（CVE-2011-1454）、Google Chrome 8.0.552.215 之前版本双重释放漏洞（CVE-2010-4494）、Google Chrome 8.0.552.215 之前版本拒绝服务漏洞（CVE-2010-4490）和 Google Chrome 8.0.552.215 之前版本不完整黑名单漏洞（CVE-2010-4487）”的综合评级为“高危”。目前，Google 已经发布了这些漏洞的补丁，CNVD 提醒广大用户及时下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05272>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05271>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05269>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05216>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05213>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05212>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05209>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05204>

2、Cisco 产品安全漏洞

Cisco Unified Communications Manager 是一款 Cisco IP 电话解决方案中的呼叫处理组件；Cisco Wireless LAN Controller 是用于使用轻量级接入点协议(LWAPP)管理 Cisco Aironet 接入点的应用设备。Cisco IOS 是一款操作系统。本周，上述 Cisco 的产品存在多个安全漏洞。CNVD 收录的相关漏洞包括：Cisco Unified Communications Manager SQL 注入漏洞（CVE-2011-1610、CVE-2011-1609）、Cisco Wireless LAN Controller ICMP 报文处理拒绝服务漏洞、Cisco Unified Communications Manager（CVE-2011-1607）目录遍历漏洞、Cisco Unified Communications Manager 拒绝服务漏洞（CVE-2011-1604、CVE-2011-1605、CVE-2011-1606）、Cisco IOS OCSP 吊销证书安全漏洞。远程攻击者可以利用漏洞绕过限制访问受限资源、使服务崩溃或通过 SQL 注入修改配置、删除或创建用户等。其中，Cisco Unified Communications Manager SQL 注入漏洞（CVE-2011-1610、CVE-2011-1609）的综合评级为“高危”。目前，厂商已经发布了这些漏洞的补丁程序，CNVD 建议广大用户及时下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05265>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05238>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05237>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05236>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05235>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05233>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05232>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05231>

3、Microsoft 产品安全漏洞

Microsoft Windows Media Player 是一款微软开发的媒体播放程序；Microsoft Internet Explorer 是流行的 WEB 浏览器。本周，Microsoft 上述两款产品均出现了安全漏洞，攻击者可以利用漏洞进行恶意欺骗，或执行任意代码，使应用程序崩溃。CNVD 收录的相关漏洞包括：Microsoft Windows Media Player 远程拒绝服务漏洞、Microsoft Internet Explorer 存在状态栏伪造漏洞。目前，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-2011-05188>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05187>

4、PHP 'phar/tar.c'堆缓冲区溢出漏洞

PHP 是一款流行的编程语言。本周，PHP 'phar/tar.c'文件存在一个整数溢出漏洞，可导致堆溢出。攻击者可以利用漏洞执行任意代码、绕过安全限制或取得较高权限。目前，互联网上已经出现针对这个漏洞的攻击代码，影响 PHP 多个版本。厂商尚未发布这个漏洞的补丁，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-2011-05182>

小结：本周，Google Chrome 存在多个安全漏洞，攻击者可以利用漏洞发起拒绝服务、执行伪造攻击，绕过同源策略，执行任意代码，获取敏感信息。PHP 产品存在一个缓冲区漏洞，且其攻击代码已在互联网上公开，对使用该产品的用户构成较大威胁。此外，Cisco、Microsoft 产品均出现了多个安全漏洞。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、HP 发布升级程序，修补多个产品安全漏洞

本周，HP 发布升级程序，修补了 SiteScope 和 Network Automation 存在的多个安全漏洞。HP SiteScope 是用于分布式 IT 基础设施功能和性能监测的解决方案；HP Network Automation 是一款自动化网络配置管理工具。攻击者利用漏洞可以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/3666>

<http://www.cnvd.org.cn/patch/3665>

<http://www.cnvd.org.cn/patch/3668>



本周要闻速递

1、WordPress 发布最新版本 修复安全漏洞

本周，WordPress 发布官方声明称，WordPress 3.1.2 已经发布，这是针对先前所有版本的一次安全更新。此版本解决了一个允许贡献者（Contributor-level）身份用户发布日志的安全漏洞。WordPress 建议您更新至 3.1.2 版本，尤其是如果允许读者以“贡献者”身份注册或者有不信任的用户。这个版本也修复了一些在 3.1.1 版本中没有来得及修复的 bug。WordPress 3.1.2 已经提供了下载和后台管理控制面板更新两种方式。

参考链接：<http://www.7747.net/News/201104/88902.html>

2、苹果承诺发布软件升级 修复位置跟踪漏洞

北京时间 5 月 3 日凌晨消息，苹果上周承诺将发布一个软件升级来解决 iOS 移动操作系统存在的地理位置跟踪漏洞问题，而根据苹果周一发给部分媒体的预览版 iOS 4.3.3 判断，该公司应该很快会发布之前承诺的软件升级。据接到预览版 iOS 4.3.3 的美国科技博客 Boy Genius Report 透露，苹果可能会在未来两周内发布这个软件升级，发布日期有可能还会提前。知情人士告诉 Boy Genius Report，在安装了该软件升级后，用户在对 iPhone 或 3G 版 iPad 进行同步操作时，iOS 4 就不会再将地理位置数据库文件“consolidated.db”备份到 iTunes 上。苹果还将像之前承诺的那样减小 consolidated.db 文件大小，限制保存地理位置数据的持续时间。苹果还承诺，当用户选择关闭其 iOS 设备上的地理位置服务时，该公司即将发布还将删除 consolidated.db 文件。除了平息与地理位置数据有关的争议之外，这个软件升级还能提高电池续航能力，修复与 iPod 软件有关的一些漏洞。

参考链接：<http://www.7747.net/News/201105/89489.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