

信息安全漏洞周报

2011 年 5 月 30 日-2011 年 6 月 5 日

2011年第22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 100 个，其中高危漏洞 37 个、中危漏洞 55 个、低危漏洞 4 个。上述漏洞中，可利用来实施远程攻击的漏洞有 87 个。网上已经出现针对“Microsoft Windows Live Messenger 'dwmapi.dll' DLL 装载任意代码执行漏洞”和“Golden FTP PASS 命令堆栈缓冲区溢出漏洞”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 46 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 家成员单位以及中国电力科学研究院信息安全实验室报送了本周收录的全部 100 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、东软、绿盟科技报送的数量较多；中国电力科学研究院信息安全实验室报送了 4 个私有漏洞，目前 CNVD 正在验证及评估漏洞危害情况，完成验证后将择时公布。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	49	0
绿盟科技	6	0
恒安嘉新	45	0
东软	5	0
安氏领信	2	0
安天	1	0
中国电力科学研究院 信息安全实验室	4	4
总计	100（去重）	4

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 Cisco、SmarterTools、Wireshark、HP、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	Cisco	8	8%
2	SmarterTools	6	6%
3	Wireshark	5	5%
4	Apache	3	3%
5	HP	2	2%
6	Linux	2	2%
7	IBM	1	1%
8	Joomla!	1	1%
9	Microsoft	1	1 %
10	其他	71	71%

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、Cisco 产品安全漏洞

Cisco Unified IP Phone 是思科的统一 IP 电话解决方案；Cisco Media Experience Engine 是思科推出的媒体体验引擎；Cisco AnyConnect Secure Mobility Client 是思科提供的远端存取解决方案，是思科的下一代 VPN 客户端。本周，上述 Cisco 产品存在多个安全漏洞。攻击者可以利用漏洞绕过安全限制，提升特权，获取敏感信息或执行任意代码。CNVD 收录的相关漏洞包括：Cisco Unified IP Phones 7900 系列签名校验绕过漏洞、Cisco Unified IP Phones 7900 系列本地特权提升漏洞（CVE-2011-1603、CVE-2011-1602）、Cisco Media Experience Engine 5600 默认验证信息验证绕过漏洞、Cisco CNS Network Registrar 默认验证信息验证绕过漏洞、Cisco AnyConnect Secure Mobility Client 本地特权提升漏洞、Cisco AnyConnect Secure Mobility Client 任意代码执行漏洞（CVE-2011-2040、CVE-2011-2039）。除“Cisco Unified IP Phones 7900 系列签名校验绕过漏洞、Cisco Unified IP Phones 7900 系列本地特权提升漏洞（CVE-2011-1603、CVE-2011-1602）”外，其余漏洞的综合评级均为“高危”。厂商已经发布了这些漏洞的补丁程序，CNVD 提醒相关用户请及时获取补丁程序进行修补。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05669>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05668>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05667>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05666>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05665>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05664>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05663>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05662>

2、Wireshark 产品安全漏洞

Wireshark 是一款开源的网络协议分析工具。本周, Wireshark 被披露存在多个安全漏洞, 攻击者可以利用漏洞对应用程序进行拒绝服务攻击。CNVD 收录的相关漏洞包括: Wireshark 处理可视网络文件存在漏洞、Wireshark 处理压缩截获数据存在漏洞、Wireshark 处理 snop 文件存在漏洞、Wireshark 处理直径字典文件存在漏洞、Wireshark 处理畸形报文时存在漏洞。目前, 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-2011-05681>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05680>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05679>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05678>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05677>

3、HP 产品安全漏洞

HP LoadRunner 是惠普公司开发的性能测试工具; H3C Intelligent Management Center 是惠普公司发行的智能管理应用程序。本周, HP 的上述产品出现了两个缓冲区溢出漏洞。攻击者可以利用漏洞以 SYSTEM 用户上下文执行任意代码, 导致应用程序崩溃。CNVD 收录的漏洞包括: HP LoadRunner 虚拟用户脚本文件远程缓冲区溢出漏洞、HP 3COM/H3C Intelligent Management Center 'img.exe' 远程堆缓冲区溢出漏洞。目前, 厂商尚未发布这两个漏洞的补丁程序, 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-2011-05673>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05654>

4、Microsoft Windows Live Messenger 'dwmapi.dll' DLL 装载任意代码执行漏洞

Microsoft Windows Live Messenger 是一款即时通信工具。Microsoft Windows Live Messenger 'dwmapi.dll' 以不安全方式装载 DLL 库, 攻击者可以诱使用户在远程 WebDAV 或 SMB 共享上打开 .plsk 文件, 以用户上下文装载任意库文件。互联网上已经出现针对该漏洞的攻击代码, 主要影响 Microsoft Windows Live Messenger 14.0、14.0.8117.416、14.0.8089 三个版本。目前, 微软尚未发布这个漏洞的补丁程序, 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-2011-05658>

5、Golden FTP PASS 命令堆栈缓冲区溢出漏洞

Golden FTP Server 是一款 Windows 平台 FTP 服务器。Golden FTP PASS 命令存在堆栈缓冲区溢出漏洞，允许恶意用户利用 PASS 命令触发缓冲区溢出。远程攻击者可利用此漏洞获取敏感信息。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 Golden FTP 4.70 版本。厂商尚未发布该漏洞的补丁程序，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-2011-05697>

小结：本周，CNVD 收录了 Cisco 产品 Unified IP Phone、Media Experience Engine、AnyConnect Secure Mobility Client 的多个安全漏洞，攻击者可以利用漏洞绕过安全限制，提升特权，获得敏感信息或执行任意代码。Wireshark 产品和 HP 产品被披露存在多个安全漏洞。同时，CNVD 还收录了 Microsoft Windows 任意代码执行漏洞以及 Golden FTP 堆栈缓冲区溢出漏洞等零日漏洞，对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個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、IBM 发布升级程序，修补 Tivoli Management Framework 安全漏洞

IBM Tivoli Management Framework 是一款网络管理基础平台。本周，IBM 发布升级程序，修补了 Tivoli Management Framework 存在的安全漏洞。远程攻击者可以利用漏洞以 SYSTEM 用户上下文执行任意代码。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/3980>

本周要闻速递

1.黑客公开火狐“魔镜”漏洞攻击方法 火狐称漏洞已修复

近日，火狐浏览器被发现存在严重的安全漏洞，其“火狐魔镜”插件出现一个高危 0day 漏洞，影响几乎所有火狐中国版浏览器用户。现在，在某些技术论坛上，已有黑客公开了火狐“魔镜”漏洞的攻击方法，火狐浏览器用户也因此面临严重的安全隐患。据悉，该漏洞对用户的影响表现为当用户误访问恶意网页，并使用“魔镜”拖拽该网页上的文字时，网站便可利用“魔镜”的漏洞注入恶意脚本，对用户电脑进行攻击。目前，火狐官方声称，已诊断出此漏洞并提供了修复。附件组件“魔镜”的更新已经通过测试，并已部署上线，最新“魔镜”版本为 4.0.2。

参考链接: <http://www.honhei.cn/News/201106/92563.html>

2. Adobe 警告用户 Flash 出现新安全漏洞

据美国媒体报道, Adobe 6 月 6 日向 Android 设备、Windows、个人电脑、Linux 和 Solaris 的用户发出警告: Flash 10.3 出现一种新的安全漏洞。该漏洞将使得恶意软件有可能随意操纵用户的电脑或 Android 设备。如果用户的设备受到恶意软件的影响, 恶意软件将可进入其网页、窃用其邮件和进入其设备的各种应用程序。Adobe 称有报道显示, 恶意软件是通过邮件中的链接展开有目的性侵袭的。对于该问题的解决, Adobe 称用户可以更新最新补丁的 Flash 应用软件。另外, Android 设备用户也可以从 Android Market 下载最新版的 Flash 应用软件。

参考链接: <http://tech.163.com/11/0607/03/75TQ2564000915BD.html>

3. 西门子被披露存在新安全漏洞

5 月中旬, 两名独立安全测评员和 NSS Labs 发现西门子的工业控制系统存在安全漏洞。SCADA (数据采集与监视控制系统) 是广泛应用在西门子 PLC 上的软件。他们发现 SCADA 存在安全漏洞, StuxnetWorm (业内人士称为超级工厂病毒、震网等) 可以很容易侵入, 黑客可以利用漏洞编写恶意软件进行攻击。上述漏洞得到了美国国土安全部的确认, NSS Labs 正积极和美国国土安全部的有关部门共同讨论如何解决这个问题。StuxnetWorm 在去年大爆发时, 我国曾有上千家工厂受到攻击。由于西门子公司生产的 PLC (programmable logic controller 可编程序控制器) 在我国的应用相当广泛, 这一新漏洞被发现再次引起业界的担心。对此, 西门子在官网上发布声明称“问题主要是随着因特网应用产生的”, 西门子自动化设备受到攻击后, 产生的故障和停电产生的故障类似。西门子中国并未直接给予回复, 称“一切均以总公司的官方声明为准”。

参考链接: <http://tech.163.com/11/0607/03/75TQ2564000915BD.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