

信息安全漏洞周报

2011 年 6 月 27 日-2011 年 7 月 3 日

2011年第26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 76 个,其中高危漏洞 37 个、中危漏洞 32 个、低危漏洞 7 个。上述漏洞中,可利用来实施远程攻击的漏洞有 68 个。网上已经出现针对“HP Operations Manager 'Register'请求任意文件删除漏洞”、“OpenSSH 'pam_thread()'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 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 7 家成员单位报送了本周收录的全部 76 个漏洞,各单位报送情况如表 1 所示。其中,启明星辰、绿盟科技报送的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	50	0
绿盟科技	80	0
恒安嘉新	5	0
东软	3	0
安氏领信	4	0
安天	1	0
知道创宇	1	0
总计	76 (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 Nullsoft、Google、Asterisk、HP、Linux 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	NullSoft	11	14.5%
2	Google	8	10.5%
3	Asterisk	4	5.3%
4	HP	3	3.9%
5	IBM	3	3.9%
6	Novell	3	3.9%
7	Linux	3	3.9%
8	Opera Software	2	2.6%
9	Comsenz Inc.	2	2.6%
10	Apache	1	1.3%
11	其他	36	47.6%

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、NullSoft Winamp 安全漏洞

Winamp 是一款媒体播放器。本周，Winamp 被披露存在多个综合评级为“高危”的安全漏洞，远程攻击者可以利用漏洞以应用程序安全上下文执行任意代码或使应用程序崩溃。CNVD 收录的相关漏洞包括：Winamp 解析 MTrk 块时 in_mod.dll 存在漏洞、Winamp 处理"Note On"消息时 in_mod.dll 存在漏洞、Winamp in_mod.dll 缓冲区溢出漏洞、Winamp in_mod.dll 内存破坏漏洞、Winamp nsvdec_vp3.dll 缓冲区溢出漏洞、Winamp nsvdec_vp6.dll 内存破坏漏洞、Winamp 缓冲区溢出漏洞等。目前，互联网上已经出现部分漏洞的攻击代码，主要影响 NullSoft Winamp 5.61 版本。厂商尚未发布升级程序修补上述漏洞，CNVD 提醒广大 Winamp 用户随时关注厂商主页以获取最新版本。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-06066>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06065>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06063>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06061>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06060>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06059>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06057>

2、Google Chrome 安全漏洞

Google Chrome 是一款 WEB 浏览器。本周，Google Chrome 被披露存在多个安全漏洞。远程攻击者可以利用漏洞使应用程序崩溃，读取敏感内存信息或执行任意代码。CNVD 收录的相关漏洞包括：Google Chrome 内存错误引用漏洞（CVE-2011-2351）、Google Chrome HTML 解析器存在漏洞（CVE-2011-2350）、Google Chrome 内存错误引用漏洞（CVE-2011-2349）、Google Chrome 错误边界检查漏洞（CVE-2011-2348）、Google Chrome 内存破坏漏洞（CVE-2011-2347）、Google Chrome 内存错误引用漏洞（CVE-2011-2346）、Google Chrome 越界读漏洞（CVE-2011-2345）。上述漏洞的综合评级均为“高危”。目前，Google 已经发布升级程序修补这些漏洞，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-2011-06089>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06088>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06086>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06083>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06082>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06081>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06080>

3、Asterisk 产品安全漏洞

Asterisk 是一款开放源码的电话系统（即 PBX）软件，支持多种 VoIP 协议和设备。本周，CNVD 收录了 Asterisk 产品存在的多个安全漏洞。CNVD 收录的 Asterisk 漏洞包括：Asterisk SIP 验证请求用户枚举漏洞、Asterisk 'iax2_setoption()' 远程拒绝服务漏洞、Asterisk 'get_in_brackets_full()' 远程拒绝服务漏洞、Asterisk 'sipsock_read()' 远程拒绝服务漏洞。上述漏洞中，“Asterisk 'get_in_brackets_full()' 远程拒绝服务漏洞”和“Asterisk 'sipsock_read()' 远程拒绝服务漏洞”的综合评级为“高危”。目前，厂商已经发布这些漏洞的修补程序，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-2011-06093>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06048>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06047>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06045>

4、HP 产品安全漏洞

HP OpenView Operations 是一款分布式客户机/服务器软件产品，用于管理分布式环境；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。本周，上述产品被披露存在多个安全漏洞。攻击者可以利用漏洞以 SYSTEM 权限删除系统文件或以应用程序上下文执行任意代码。CNVD 收录的相关漏洞包括：

HP Operations Manager 'Register'请求任意文件删除漏洞、HP OpenView Storage Data Protector 未明远程代码执行漏洞（CVE-2011-1865、CVE-2011-1186）。目前，互联网上已经出现针对“HP Operations Manager 'Register'请求任意文件删除漏洞”的攻击代码，主要影响 HP Operations Manager 8.1 版本。除该漏洞外，HP 已经发布其余漏洞的修补程序，CNVD 提醒广大 HP 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-2011-06078>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06076>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06074>

5、OpenSSH 'pam_thread()'远程缓冲区溢出漏洞

OpenSSH 是一款 SSH 协议开放源代码实现。本周，OpenSSH 被披露存在一个预验证缓冲区溢出漏洞，远程攻击者可以利用漏洞以 root 权限执行任意代码。目前，互联网上已经出现了针对该漏洞的攻击代码，主要影响 OpenSSH 3.5p1 版本。此漏洞的综合评级为“高危”。厂商尚未发布该漏洞的修补程序，CNVD 提醒相关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-2011-06107>

小结: 本周, NullSoft Winamp 和 Google Chrome 被披露存在多个综合评级为“高危”的安全漏洞，攻击者可以利用漏洞远程执行任意代码或使应用程序崩溃，对使用上述产品的用户构成较为严重的威胁。同时, Asterisk 和 HP 产品也出现了多个安全漏洞。此外，OpenSSH 零日漏洞也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、Linux 发布升级程序，修补 Kernel 多个安全漏洞

本周，Linux 发布升级程序，修补 Kernel 的多个安全漏洞。远程攻击者可以利用漏洞获得敏感内核信息或使应用程序崩溃。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/4247>
<http://www.cnvd.org.cn/patch/4271>



本周要闻速递

1. 测试版本 Chrome+存在安全漏洞

北京时间 7 月 1 日消息，正处在测试版本的 Google+ 被曝出存在安全漏洞，用户可以利用这个安全漏洞与其他任何人分享其他用户发布的内容。根据报告称，这可能与 Google+ 的邀请方式有关。一名报社记者蒂姆·布拉德肖 (Tim Bradshaw) 发现了 Google Plus 的隐私问题，尽管他表示这个问题并没有造成严重后果，但是这个共享选项的漏洞，还是给谷歌创造一个尊重隐私的社交平台的想法蒙上了阴影。这个分享键一旦被选中，就会将这个信息分享给谷歌圈内人 (Google+ Circles)。如果用户是真的想去分享这个内容，那么不会有什么影响，但是如果这个内容的发布者仅仅希望在有限的圈子内分享的话呢？布拉德肖还指出：“我的一个朋友将孩子的照片贴到了自己的朋友圈里面。由于 Google+ 的分享选项，我可以把这些照片分享给任何一个人，也可以把这些照片贴到我朋友不在的那些圈子里边，这样这些照片就可能会被任何人看到。这个漏洞并不仅仅限于照片的分享。”根据 Bradshaw 的报告，谷歌已获悉他所指出的漏洞，并作出了回应，称这正是开发测试阶段需要做的工作--寻找和修正 bug。

参考链接：<http://www.enet.com.cn/article/2011/0704/A20110704879895.shtml>

2. 苹果已封堵开发者网站 0day 漏洞

据报道，曾有新闻报导了外国著名的黑客组织 YGN Ethical 在苹果开发者网站上发现安全漏洞的消息。YGN 指出，该漏洞可能会导致 Mac OS X 以及 iOS 开发者陷入钓鱼诈骗。在请求苹果对此进行修复不果之后，YGN 遂将此事公布于众。据最新消息透露，日前苹果已成功对该漏洞进行封堵。据了解，YGN 曾在今年 4 月 25 日向苹果反应，开发者网站上出现“任意 URL 重定向”安全漏洞，虽然苹果于两天后公开承认该漏洞的存在，但是却不对其进行修复。随后 YGN 将此事公之于众，在媒体压力之下苹果很快就对该漏洞进行了封堵。有媒体称，由于美国法律规定，未经授权的浏览可以被归为“侵犯”又或甚至是“恶意攻击”，所以 YGN 的行为也引起许多网友的争议。不过这个黑客组织认为，任何一个网站都不应该出现危及用户权益的漏洞，尤其是那些知名企业的网站。在今年早些时候，YGN Ethical 黑客组织也曾在 MaAfee 以及甲骨文公司网站上发现安全漏洞。

参考链接：<http://iphone.tgbus.com/news/class/201107/20110703105329.shtml>

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