

信息安全漏洞周报

2011 年 6 月 6 日-2011 年 6 月 12 日

2011年第23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 38 个、中危漏洞 39 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 75 个。网上已经出现针对“Xitami HTTP 头远程缓冲区溢出漏洞”、“1 Click Unzip! '.zip'文件堆缓冲区溢出漏洞”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 68 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 80 个漏洞，各单位报送情况如表 1 所示。其中，启明星辰、东软、绿盟科技报送的数量较多。另外，知道创宇公司报送了网御神州官方网站存在 sql 注入漏洞，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。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	74	0
绿盟科技	7	0
恒安嘉新	6	0
东软	17	0
安氏领信	2	0
知道创宇	1	1
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 Sun、Google、Novell、HP、VMWare 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	Sun	17	21.3%
2	Google	14	17.5%
3	Novell	10	12.5%
4	HP	8	10.0%
5	VMWare	4	5.0%
6	ACD Systems	3	3.8%
7	Autonomy	2	2.5%
8	IBM	1	1.3%
9	Adobe	1	1.3%
10	Wordpress	1	1.3%
11	其他	19	24.8%

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、Sun 产品安全漏洞

Oracle 发布了 2011 年 6 月的安全公告，修补了 Sun Java SE 平台中存在的 17 个安全漏洞。其中 9 个漏洞的综合评级为“严重”（CVSS 评分为 10）。利用上述漏洞，远程攻击者可以执行任意代码或进行拒绝服务攻击，对相关用户构成较为严重的威胁。CNVD 收录的相关漏洞包括：Sun Java Runtime Environment 组件任意代码执行漏洞（CVE-2011-0866）、Sun Java 部署组件任意代码执行漏洞（CVE-2011-0788、CVE-2011-0786）、Sun Java Swing 组件任意代码执行漏洞（CVE-2011-0871）、Sun Java 声音组件任意代码执行漏洞（CVE-2011-0814、CVE-2011-0802）、Sun Java HotSpot 组件任意代码执行漏洞（CVE-2011-0864）、Sun Java 部署组件任意代码执行漏洞（CVE-2011-0863、CVE-2011-0817）、Sun Java AWT 组件任意代码执行漏洞（CVE-2011-0815）、Sun Java 2D 组件任意代码执行漏洞（CVE-2011-0862、CVE-2011-0873）等。上述漏洞的综合评级均为“高危”。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-2011-05809>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05803>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05802>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05801>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05800>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05799>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05798>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05797>

2、Google 产品安全漏洞

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，或绕过同源策略获得敏感信息。CNVD 收录的相关漏洞包括：Google Chrome 同源绕过漏洞（CVE-2011-2342、CVE-2011-2332）、Google Chrome 扩展注入漏洞（CVE-2011-1819）、Google Chrome 内存引用错误漏洞（CVE-2011-1818、CVE-2011-1816）、Google Chrome 内存破坏漏洞（CVE-2011-1817）、Google Chrome 扩展脚本注入漏洞（CVE-2011-1815）、Google Chrome 未初始化指针引用漏洞（CVE-2011-1814）、Google Chrome 引用旧指针漏洞（CVE-2011-1813）等。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-2011-05778>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05777>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05776>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05775>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05774>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05770>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05769>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05768>

3、Novell iPrint Client 安全漏洞

Novell iPrint Client 打印解决方案允许用户向网络打印机发送文档。本周，Novell iPrint Client 被披露存在多个远程代码执行漏洞。远程攻击者可以利用漏洞以浏览器上下文执行任意代码。CNVD 收录的漏洞包括：Novell iPrint Client 远程代码执行漏洞（CVE-2011-1708、CVE-2011-1707、CVE-2011-1706、CVE-2011-1705、CVE-2011-1704、CVE-2011-1703、CVE-2011-1702、CVE-2011-1701、CVE-2011-1700、CVE-2011-1699）。上述漏洞的综合评级均为“高危”。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-2011-05749>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05748>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05747>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05746>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05745>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05744>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05743>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05742>

4、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 Service Manager 是一款 IT 服务管理解决方案。本周，上述 HP 的产品被披露存在多个安全漏洞。攻击者可以利用漏洞执行任意脚本代码，进行未经授权访问或获取敏感信息。CNVD 收录的相关漏洞包括：HP OpenView Storage Data Protector 未明远程代码执行漏洞、HP Service Manager 和 Service Center 脚本注入漏洞（CVE-2011-1863）、HP Service Manager 和 Service Center 任意代码执行漏洞（CVE-2011-1862）、HP Service Manager 和 Service Center 未经授权访问漏洞（CVE-2011-1861）、HP Service Manager 和 Service Center 会话验证重用漏洞（CVE-2011-1860）、HP Service Manager 和 Service Center 获取特权漏洞（CVE-2011-1859）、HP Service Manager 和 Service Center 本地数据访问漏洞（CVE-2011-1858）、HP Service Manager 和 Service Center 未经授权访问漏洞（CVE-2011-1857）。其中，“HP Service Manager 和 Service Center 脚本注入漏洞（CVE-2011-1863）、HP Service Manager 和 Service Center 未经授权访问漏洞（CVE-2011-1861）、HP Service Manager 和 Service Center 未经授权访问漏洞（CVE-2011-1857）”的综合评级为“高危”。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-2011-05812>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05792>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05791>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05790>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05789>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05788>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05787>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05786>

5、Xitami HTTP 头远程缓冲区溢出漏洞

Xitami 是一款 Web 服务软件。Xitami 未能正确处理特制的 HTTP 头字段数据，攻击者可以利用漏洞提交恶意请求触发缓冲区溢出，成功利用漏洞可以以应用程序安全上下文执行任意代码。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 Imatix Xitami 2.5b4 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-2011-05758>

小结：本周，Oracle 发布了 2011 年 6 月的安全公告，修补了 Sun Java SE 平台中存在的 17 个安全漏洞。远程攻击者可利用漏洞执行任意代码或进行拒绝服务攻击，对用户构成

较为严重的威胁。Google、Novell、HP 产品被披露存在多个安全漏洞，此外，Xitami 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、VMware 发布升级程序，修补多个产品安全漏洞

本周，VMware 发布升级程序，修补 ESXi 和 ESX Server 产品的多个安全漏洞。远程攻击者可以利用漏洞获取敏感信息、绕过安全限制或提升特权。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/4033>

<http://www.cnvd.org.cn/patch/4034>

<http://www.cnvd.org.cn/patch/4035>

<http://www.cnvd.org.cn/patch/4036>

本周要闻速递

1、西门子（中国）网站发布漏洞提示

近日，西门子存在漏洞的相关产品说明的中文版本已经放在西门子（中国）工业自动化与驱动计划网站上，西门子很多使用者都会浏览这个网站，应该可以看到相关信息。据西门子（中国）官方网站资料，漏洞产品 S7-1200 的固件更新将在 6 月提供。固件更新将会提供弥补措施，此固件针对重放攻击加强了保护措施，同时增强了 S7-1200 在面对上述拒绝服务攻击时的稳定性。此信息的发布比其英文版本晚了 13 天。西门子（中国）表示，到目前为止，他们还没有接到任何客户就此问题的质询。网络攻击只有在下述非常极端的条件下才会发生：即入侵者必须在工厂现场或者可以任意访问生产网络。即便受到网络攻击，CPUS7-1200 的反应将是切换到停机/故障状态，并将自动化过程置于安全模式。如果确实有必要，或许将对中国使用者进行提示。

参考链接：<http://www.honhei.cn/News/201106/93253.html>

2、我国检测发现 Adobe Flash Player 零日漏洞

国家计算机病毒应急处理中心通过对互联网的监测发现，Adobe Flash Player 在实现上存在跨站脚本执行漏洞，即“零日”漏洞。专家说，恶意远程攻击者可利用此漏洞在受影响的 Web 站点浏览器中执行任意代码指令，窃取临时文件 Cookie 身份验证凭证，发动其他恶意入侵攻击。如果计算机用户使用 Flash Player 的版本是 10.3.181.16 或早期的，需要下载更新版本至 10.3.181.22 或以上的版本来弥补该漏洞。除此之外，该升级版本补丁程序还考

考虑到 Adobe 的每月正常更新问题，以避免再次发生之前出现过的其插件受到恶意攻击的情况。Adobe 公司已经为此发布了一个安全公告（APSB11-13）以及相应补丁程序 APSB11-13（Security update available for Adobe Flash Player），专家建议计算机用户可以通过访问 Adobe 的版本检测网站来检查升级安装 Flash Player 的最新版本，也可以自动或手动安装。

参考链接：http://news.xinhuanet.com/newmedia/2011-06/12/c_121524458.htm

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