

信息安全漏洞周报

2011 年 7 月 18 日-2011 年 7 月 24 日

2011年第29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**高**。

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 125 个，其中高危漏洞 37 个、中危漏洞 75 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 104 个。网上已经出现针对“Freefloat FTP Server MKD 缓冲区溢出漏洞”、“WordPress WP e-Commerce 插件'wpesc-user_log_functions.php' SQL 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 108 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，5 家成员单位报送了本周收录的全部 125 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、恒安嘉新报送的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	140	0
绿盟科技	56	0
恒安嘉新	39	0
安氏领信	2	0
东软	9	0
总计	125（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 Oracle、Apple、Google、Cisco、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	Oracle	56	44.8%
2	Apple	15	12.0%

3	Enano	8	6.4%
4	WebKit Open Source Project	8	6.4%
5	Western Digital	5	4.0%
6	Cisco	3	2.4%
7	IBM	2	1.6%
8	Google	1	0.8%
9	Baidu	1	0.8%
10	HTC	1	0.8%
11	其他	25	20.0%

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、Apple Safari 安全漏洞

Apple Safari 是一款 WEB 浏览器。本周，Apple 发布安全公告，修复了 Safari 存在多个安全漏洞。远程攻击者可以利用漏洞窃取敏感信息或执行任意代码。CNVD 收录的相关漏洞包括：Apple Safari CFNetwork 跨站脚本漏洞、Apple Safari CFNetwork NTLM 验证协议远程代码执行漏洞、Apple Safari 'libxml'远程代码执行漏洞、Apple Safari ImageIO TIFF 图像处理堆缓冲区溢出漏洞、Apple Safari CFNetwork Root 证书安全绕过漏洞、Apple Safari 'AutoFill web forms'功能信息泄露漏洞、Apple Safari 跨域信息泄露漏洞、Apple Safari 存在多个内存破坏漏洞。其中，“Apple SafariCFNetwork NTLM 验证协议远程代码执行漏洞、Apple Safari 'libxml'远程代码执行漏洞、Apple Safari ImageIO TIFF 图像处理堆缓冲区溢出漏洞”的综合评级为“高危”。CNVD 提醒广大 Apple 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-2011-06443>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06440>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06439>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06438>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06436>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06434>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06430>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06429>

2、WebKit 安全漏洞

WebKit 是一款开源的浏览器引擎。本周，WebKit 被披露存在多个安全漏洞。攻击者可以利用漏洞发起执行任意代码、跨站脚本攻击。CNVD 收录的相关漏洞包括：WebKit 'libxslt' 远程代码执行漏洞、WebKit SVG 标签 'animVal' 属性远程代码执行漏洞、WebKit 嵌入 URL 跨域脚本漏洞、WebKit 畸形 XHTML 标签内存破坏漏洞、WebKit MathML 标签远程代码执行漏洞、WebKit 畸形 TIFF 图像内存破坏漏洞、WebKit Frameset 元素内存破坏漏洞。上述漏洞中，除“WebKit 嵌入 URL 跨域脚本漏洞”外，其余漏洞的综合评级均为“高危”。目前，厂商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-2011-06444>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06442>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06441>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06424>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06422>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06421>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06411>

3、Oracle 产品安全漏洞

本周，Oracle 发布了 2011 年 7 月的安全更新，修复了 Oracle Database、Fusion Middleware、Enterprise Manager Suite、PeopleSoft、E-Business Suite、Oracle Supply Chain 和 Oracle Sun Product Suite 多个产品存在的多个安全漏洞。利用上述漏洞，攻击者可发起窃取敏感信息、提升特权、执行任意代码等攻击，甚至可以使应用程序崩溃或取得主机操作系统管理权限。CNVD 收录的相关漏洞包括：Oracle Database Server 远程 Core RDBMS 漏洞（CVE-2011-2253）、Oracle Database Server RDBMS 远程 Core RDBMS 漏洞（CVE-2011-2239）、Oracle Solaris 存在未明漏洞（CVE-2011-2287、CVE-2011-2285、CVE-2011-2245）、Oracle Secure Backup 存在未明漏洞（CVE-2011-2261）、Oracle Database Server 远程 Database Vault 漏洞（CVE-2011-2238）、Oracle Solaris 提升特权漏洞（CVE-2011-2298）等。上述漏洞中，除“Oracle Database Server 远程 Database Vault 漏洞（CVE-2011-2238）、Oracle Solaris 提升特权漏洞（CVE-2011-2298）”外，其余漏洞的综合评级均为“高危”。CNVD 提醒广大 Oracle 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-2011-06447>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06426>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06403>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06402>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06399>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06393>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06425>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06406>

4、Google Picasa JPEG 图像处理远程代码执行漏洞

Picasa 是 Google 推出的一款免费图片管理工具。Picasa 处理特制的 JPEG 图像存在安全漏洞，攻击者可以利用漏洞使 Picasa 崩溃或执行任意代码。成功利用漏洞可以当前用户上下文取得操作系统权限。目前，Google 已经发布升级程序修补这个漏洞，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-2011-06344>

5、Android HTC FTP 服务目录遍历漏洞

HTC 是一款智能手机。运行在 Android 2.1 和 Android 2.2 平台上的 HTC 设备提供的蓝牙 OBEX FTP 服务存在目录遍历漏洞，利用这个漏洞允许远程已验证攻击者通过提交../的路径名请求，列出任意目录和读取任意文件。目前，厂商尚未发布修补程序修复该漏洞，CNVD 提醒相关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-2011-06433>

6、Freefloat FTP Server MKD 缓冲区溢出漏洞

Freefloat FTP Server 是一款 FTP 服务程序。Freefloat FTP Server 处理 MKD 命令时存在缓冲区溢出漏洞，远程攻击者可利用此漏洞使应用程序崩溃或以应用程序上下文执行任意代码。此漏洞的综合评级为“高危”。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 Freefloat FTP Server 1.00 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-2011-06331>

小结：本周，Oracle 发布 2011 年 7 月安全公告，修补多个产品安全漏洞，远程或本地攻击者可以利用漏洞提升特权或执行任意代码，对使用 Oracle 产品的用户构成较为严重的威胁。同时，Apple Safari、WebKit、Google 和 HTC 产品也被披露存在多个安全漏洞。此外，Freefloat FTP Server 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、IBM 发布升级程序，修补 WebSphere Application Server 安全漏洞

本周，IBM 发布升级程序，修补了 IBM WebSphere Application Server 存在的多个安全漏洞。攻击者可以利用漏洞绕过安全限制或获得敏感信息。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/4430>
<http://www.cnvd.org.cn/patch/4431>

本周要闻速递

1. 苹果修复了 Safari 浏览器漏洞

据国外媒体报道，苹果日前发布了 Safari 浏览器几个关键安全漏洞的补丁。本周三苹果发布公告解决 Windows 和 Mac 上 Safari 5.1 和 5.06 的几个安全漏洞。公告中指出 Safari 的 23 个问题和约 58 个漏洞，主要漏洞将影响使用 Windows、Vista、XP SP2 及之后颁布的台式 Mac 电脑。此次列出的漏洞包括跨站脚本漏洞、可能被黑客用于控制系统的缓冲区及整数溢出等，其中 2 个问题会影响 Mac OS X 和 Mac OS X 服务器。漏洞还包括 Webkit 浏览器引擎中的多个内存损坏问题，这将使得用户访问网站时受到任意代码执行攻击。

参考链接: http://news.ccidnet.com/art/11099/20110722/2443329_1.html

2. 谷歌修复 URL 删除工具漏洞

据国外媒体报道，日前谷歌修复了 URL 删除工具中的一个重要漏洞，这个工具是让用户从谷歌搜索列表中删除内容的。谷歌称目前还没有发现利用该漏洞发起恶意攻击的行为。漏洞发现者表示通过对 URL 进行一些小改动就能够删除那些自己没有控制权的网站链接。

参考链接: http://news.ccidnet.com/art/11099/20110722/2443301_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