

信息安全漏洞周报

2011 年 7 月 4 日-2011 年 7 月 10 日

2011 年第 27 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 41 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“Pro Softnet IDrive Online Backup ActiveX 'SaveToFile()'任意文件覆盖漏洞”、“iMesh 'IMWebControl.dll' ActiveX 控件缓冲区溢出漏洞”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 61 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 5 家成员单位和 1 位个人上报者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、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	72	0
绿盟科技	44	0
恒安嘉新	28	0
东软	6	0
安天	2	0
个人上报者	2	0
总计	100（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 Opera Software、IBM、ISC、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	Opera Software	17	17%
2	IBM	6	6%
3	DotNetNuke	4	4%
4	phpMyAdmin	4	4%
5	Linux	3	3%
6	HP	3	3%
7	ISC	2	2%
8	Cisco	1	1%
9	Apple	1	1%
10	Apache	1	1%
11	其他	58	58%

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、ISC BIND 安全漏洞

Bind 是一款开源的 DNS 服务器软件。本周，BIND 产品被披露存在两个综合评级为“高危”的安全漏洞。远程攻击者可以利用漏洞使受影响的应用程序崩溃，造成拒绝服务攻击。CNVD 收录的相关漏洞包括：ISC BIND 远程拒绝服务漏洞（CVE-2011-2464）、ISC BIND 远程拒绝服务漏洞（CVE-2011-2465）。目前，ISC 已经发布升级程序修补了这些漏洞，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-2011-06159>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06157>

2、IBM 产品安全漏洞

本周，IBM 产品 InfoSphere Information Server、Tivoli Storage Manager 和 Rational DOORS 存在多个安全漏洞。本地或远程攻击者可以利用漏洞获得 root 特权、窃取敏感信息或劫持用户会话。CNVD 收录的相关漏洞包括：IBM InfoSphere Information Server 本地特权提升漏洞、IBM Tivoli Storage Manager Client 缓冲区溢出漏洞（CVE-2011-1223、CVE-2011-1222）、IBM Rational DOORS 未明漏洞、IBM Rational DOORS 服务器错误应答漏洞、IBM Rational DOORS 跨站脚本漏洞。目前，IBM 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-2011-06126>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06125>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06124>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06122>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06121>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06118>

3、Opera Web Browser 安全漏洞

Opera 是一款 WEB 浏览器。本周, Opera Web Browser 被披露存在多个拒绝服务漏洞。远程攻击者可以利用漏洞使应用程序崩溃。CNVD 收录的相关漏洞包括: Opera Web Browser 远程拒绝服务漏洞 (CVE-2011-2615、CVE-2011-2614、CVE-2011-2613、CVE-2011-2612、CVE-2011-2611) 等。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-2011-06151>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06150>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06149>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06148>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06147>

4、DotNetNuke 产品安全漏洞

DotNetNuke 是一款开源的网站内容管理系统。本周, DotNetNuke 被披露存在多个安全漏洞。远程攻击者可以利用漏洞绕过安全限制、未授权访问应用系统或执行任意代码。CNVD 收录的漏洞包括: DotNetNuke 权限授予漏洞、DotNetNuke 任意代码执行漏洞、DotNetNuke 校验用户权限漏洞、DotNetNuke 'soft-deleting'安全绕过漏洞。其中, “DotNetNuke 校验用户权限漏洞”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-2011-06179>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06177>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06175>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06172>

5、Pro Softnet IDrive Online Backup ActiveX 'SaveToFile()'任意文件覆盖漏洞

Pro Softnet IDrive Online Backup 是一款在线备份工具。本周, IDrive Online Backup 被披露存在一个综合评级为“高危”的安全漏洞。IDrive Online Backup ActiveX 控件 UniBasicPack.UniTextBox (UniBasic100_EDA1811C.ocx) 使用不安全的"SaveToFile()"方法, 允许攻击者通过诱使用户解析经恶意构建的 WEB 页, 以目标用户上下文覆盖系统文件。目前, 互联网上已经出现针对该漏洞的攻击代码, 主要影响 Pro Softnet IDrive Online Backup 3.4.0 版本。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-2011-06186>

小结: 本周, ISC BIND 被披露存在两个综合评级为“高危”的拒绝服务漏洞, 远程攻击者可以利用漏洞使受影响的应用程序崩溃, 造成拒绝服务攻击。对使用该产品的用户构成较为严重的威胁。同时, IBM 产品、DotNetNuke 产品和 Opera WEB 浏览器也被披露存在多个安全漏洞。此外, IDrive Online Backup 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、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 HP-UX 和 Intelligent Management Center 存在的安全漏洞。本地或远程攻击者可以利用漏洞提升特权、发起拒绝服务攻击或执行任意代码。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/4308>

<http://www.cnvd.org.cn/patch/4346>

本周要闻速递

1. 苹果 iOS 漏洞被预测将通过 Twitter 传播

7 月 9 日消息, 据国外媒体报道, 近日苹果 iOS 移动平台爆出新漏洞, 一家安全公司预测黑客将通过 Twitter 来利用该漏洞。该漏洞被著名黑客 Comex 发现, 他为最新版本的 iOS 系统开发了越狱工具。该工具可以允许苹果移动设备的用户下载非苹果公司许可的工具和应用。安全公司在博客中称, 黑客可能通过微博站点 Twitter 来利用该漏洞, 但黑客使用该漏洞的动机偏向于惹恼用户, 而非使恶意软件感染用户。安全公司提醒苹果用户在访问 Twitter 时要格外小心, 直到苹果公司将该漏洞修复, 预计在 iOS 4.3.4 版本中可以实现。

参考链接: <http://www.c114.net/news/551/a627586.html>

2. 微软 7 月份预修复 22 个漏洞

微软公司宣布将在下周二发布一个“危急”和三个“重要”补丁, 修复 Windows 和 Visio2003 中存在的 22 个漏洞, 前者修复 Windows Vista SP1、SP2、Windows 7 中导致黑客远程代码执行攻击的漏洞, 后者则发生在 Visio2003 Service Pack 3 上, 同样是代码执行漏洞。最近 Vista SP1 结束支持将意味着这款系统不会有更多安全更新出现, Vista 的

消费者将变得更为脆弱。

参考链接: <http://www.hackbase.com/news/2011-07-08/107716.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