

信息安全漏洞周报

2011 年 7 月 25 日-2011 年 7 月 31 日

2011年第30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 95 个,其中高危漏洞 35 个、中危漏洞 47 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 85 个。网上已经出现针对“MyWebServer 远程缓冲区溢出漏洞”、“Computer Associates ARCserve D2D 'homepageServlet' Servlet 信息泄露漏洞”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 49 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,4 家成员单位和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 9 5 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	54	0
恒安嘉新	49	0
东软	5	0
安氏领信	1	0
中国电力科学研究院 信息安全实验室	3	3
总计	95 (去重)	3

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 HP、Apple、Dlink、Linux、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	HP	5	5.3%
2	Dlink	4	4.2%

3	Joomla!	4	4.2%
4	phpMyAdmin	4	4.2%
5	EMC	3	3.2%
6	IBM	2	2.1%
7	Linux	2	2.1%
8	ICQ Inc.	2	2.1%
9	Computer Associates	1	1.1%
10	Apple	1	1.1%
11	其他	67	70.4%

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、HP 产品安全漏洞

本周，HP 的多款产品 OpenView Storage Data Protector、SiteScope 和 Network Automation 等出现了多个安全漏洞。攻击者可以利用这些漏洞进行拒绝服务攻击，使受影响应用程序崩溃；或进行跨站脚本攻击，劫持目标用户会话。CNVD 收录的相关漏洞包括：HP SiteScope 会话固定漏洞、HP Network Automation SQL 注入漏洞（CVE-2011-2403）、HP Network Automation 跨站脚本漏洞（CVE-2011-2402）、HP Linux 图像和打印不安全临时文件创建漏洞、HP OpenView Storage Data Protector 拒绝服务漏洞、HP SiteScope 跨站脚本漏洞。上述漏洞中，“HP SiteScope 会话固定漏洞、HP Network Automation SQL 注入漏洞（CVE-2011-2403）”的综合评级为“高危”。除“HP Linux 图像和打印不安全临时文件创建漏洞”外，厂商已经发布其余漏洞的补丁程序，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-2011-06526>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06519>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06521>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06473>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06539>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06524>

2、EMC 产品安全漏洞

本周，EMC 的产品 Data Protection Advisor、Captiva eInput 被披露存在多个安全漏洞。本地或远程攻击者可以利用漏洞获得敏感信息，劫持用户会话，或进行拒绝服务攻

击。CNVD 收录的相关漏洞包括：EMC Data Protection Advisor 账户信息泄露漏洞、EMC Captiva eInput ActiveX 函数不安全方法漏洞、EMC Captiva eInput 跨站脚本漏洞。其中，“EMC Data Protection Advisor 账户信息泄露漏洞、EMC Captiva eInput ActiveX 函数不安全方法漏洞”的综合评级为“高危”。目前，EMC 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-2011-06515>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06502>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06501>

3、Dlink DPH 安全漏洞

Dlink DPH 是一款 IP 电话解决方案。本周，Dlink DPH 被披露存在多个安全漏洞。主要影响的版本是 150SE/E/F1。远程攻击者可以利用漏洞绕过验证获得包括管理员密码的配置文件信息。CNVD 收录的漏洞包括：Dlink DPH 150SE/E/F1 IP Phones 设备重启漏洞、Dlink DPH 150SE/E/F1 IP Phones 消息修改漏洞、Dlink DPH 150SE/E/F1 IP Phones 文件上传漏洞、Dlink DPH 150SE/E/F1 IP Phones 信息泄露漏洞。漏洞的综合评级均为“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-2011-06486>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06484>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06483>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06482>

4、Apple iOS 数据安全证书链验证漏洞

iOS 是一款运行在苹果 iPhone 和 iPod touch 设备上的最新的操作系统。iOS 的 SSL 证书解析包含一个缺陷，它没有正确检查链中的 basicConstraints 参数，对使用一个合法的最终实体证书进行签名，攻击者可以获得任意域的“合法”证书，使用这种技术任何使用 api.someotherdomain.com 证书的 SSL 通信可被发行人截获和解密。不会对 IOS 用户提示任何证书非法的通知，这个方法允许针对加密 IOS 通信进行透明的中间人攻击。目前，Apple 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-2011-06466>

5、Computer Associates ARCserve D2D 'homepageServlet' Servlet 信息泄露漏洞

Computer Associates ARCserve Backup 是一款多平台的备份和恢复保护解决方案。本周，Computer Associates ARCserve Backup 被披露存在一个信息泄露漏洞。远程攻击者可利用此漏洞获得敏感用户名和密码信息。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 Computer Associates ARCserve D2D r15 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-2011-06470>

小结: 本周, CNVD 收录了 HP 产品的多个安全漏洞, 攻击者可以利用这些漏洞进行拒绝服务攻击, 使受影响应用程序崩溃; 或进行跨站脚本攻击, 劫持目标用户会话。同时, Apple、DLink 和 EMC 产品也被披露存在多个安全漏洞。此外, Computer Associates 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 安全漏洞

本周, Linux 发布升级程序, 修补了 Kernel 存在的多个安全漏洞。攻击者可以利用漏洞绕过安全验证获得敏感信息或使程序崩溃导致拒绝服务。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/4558>

<http://www.cnvd.org.cn/patch/4559>

<http://www.cnvd.org.cn/patch/4581>

本周要闻速递

1. Facebook 推漏洞奖励计划

据国外媒体报道, Facebook 公司将对发现其网络中安全缺陷的研究人员奖励 500 美元或更高的奖金。Facebook 发表博文称, “为了表达我们对安全研究人员的谢意, 我们将对发现某些类型安全缺陷的研究人员给予现金奖励。Facebook 表示, “首先负责任地披露可能危及 Facebook 用户数据完整性和隐私的缺陷”的研究人员将获得 500 美元奖金。Facebook 说, “我们的安全团队将对缺陷进行评估, 决定研究人员能否获奖。” Facebook 表示, 通常情况下奖金是 500 美元。

参考链接: <http://news.itxinwen.com/internet/inland/2011/0801/329704.html>

2. iOS 再爆安全漏洞

近日, 苹果 iOS 操作系统再次爆出安全漏洞。黑客能通过这个漏洞轻松截获 iOS 设备传输的数据流, 通过名为 SSLSniff 的工具即可拦截未打安全补丁的 iOS 设备通信数据。这个安全漏洞在 iOS 4.3.4 (GSM)、4.2.9 (CDMA) 以及 iOS5 测试版系统中被证实均存在。

参考链接: <http://pcedu.pconline.com.cn/ios/1107/2485513.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