

信息安全漏洞周报

2012 年 4 月 9 日-2012 年 4 月 15 日

2012 年第 15 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 108 个，其中高危漏洞 36 个、中危漏洞 70 个、低危漏洞 2 个。上述漏洞中，可利用来实施远程攻击的漏洞有 103 个。本周收录的漏洞中，已有 71 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。本周互联网上出现“NetOp 远程控制客户端缓冲区溢出漏洞”、“CitrusDB 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加强防范。

成员单位报送漏洞统计

本周，共 7 家成员单位和多个合作伙伴报送了本周收录的全部 108 个漏洞。各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰、安天实验室、天融信等单位报送数量较多。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	85	0
绿盟科技	67	0
天融信	21	0
安天实验室天	26	0
恒安嘉新	20	0
东软	3	0
安氏领信	4	0
华为	1	1
个人研究者	1	1
报送总计	228	2

总计	108（去重）	2
----	---------	---

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、RealNetworks、Puppet Labs、Adobe、Cisco 等多家厂商的产品，部分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	Microsoft	11	10.2%
2	RealNetworks	6	5.6%
3	Puppet Labs	5	4.6%
4	Adobe	4	3.7%
5	Cisco	3	2.8%
6	Siemens	3	2.8%
7	HP	2	1.9%
8	Apache	1	0.9%
9	Red Hat	1	0.9%
10	Oracle	1	0.9%
11	其它	71	65.7%

表 2 漏洞产品涉及厂商分布统计表



漏洞按影响类型统计

本周，CNVD 收录了 108 个漏洞。其中操作系统漏洞 1 个，应用程序漏洞 61 个，WEB 应用漏洞 35 个，网络设备漏洞 5 个，数据库漏洞 1 个，安全产品漏洞 5 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	1
应用程序漏洞	61
WEB 应用漏洞	35
网络设备漏洞	5
数据库漏洞	1
安全产品漏洞	5

表 3 漏洞按影响类型统计表

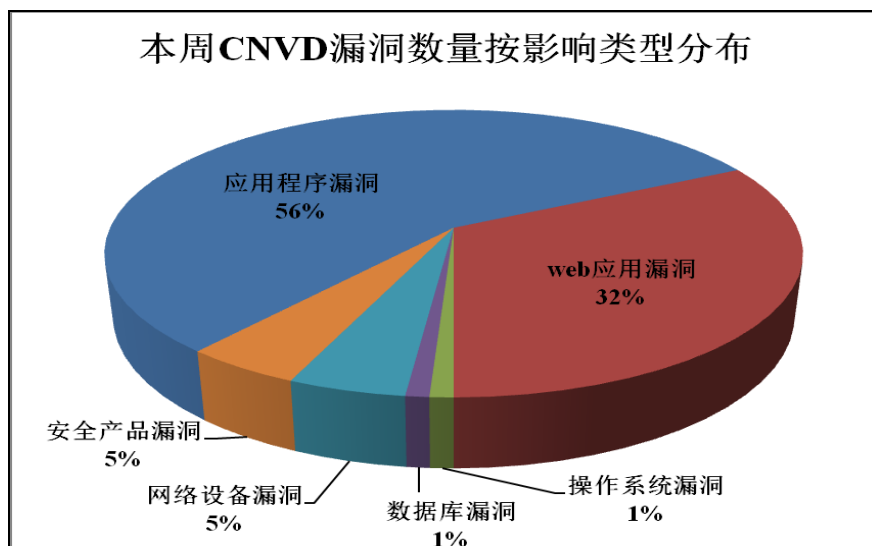


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周,CNVD 共收录了 5 个网络设备漏洞。其中,“Siemens Scalance X Switches HTTP 请求处理拒绝服务漏洞”的综合评级为“高危”;“Cisco IronPort Web Security Appliance 证书参数校验漏洞”、“Cisco IronPort Web Security Appliance 密钥对缓存漏洞”、“Cisco IronPort Web Security Appliance 证书吊销检查漏洞”和“HP ProCurve 5400 zl Switch 恶意软件感染闪存卡漏洞”的综合评级均为“中危”。

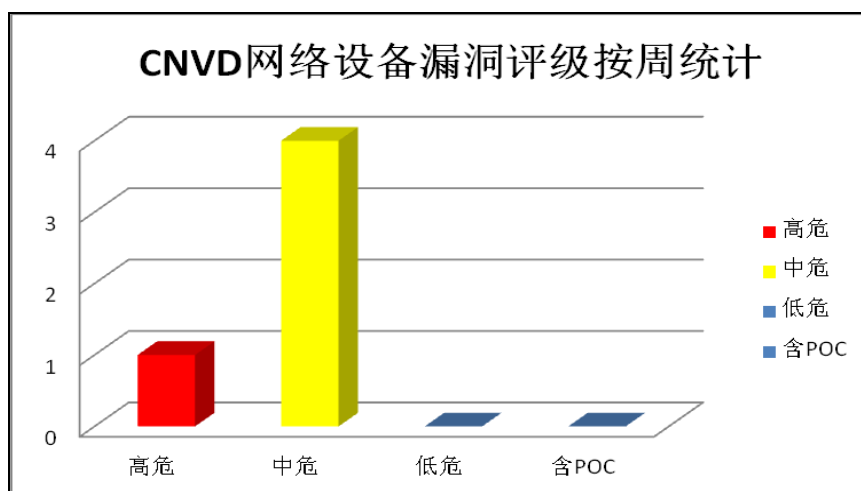


图 2 网络设备漏洞统计

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、Microsoft 产品安全漏洞

4 月 10 日, 微软发布了 2012 年 4 月份的月度例行安全公告, 共包含 6 项安全更新,

修复了涉及 Windows 操作系统、.NET Framework、Office 软件套件、Internet Explorer 浏览器、Forefront UAG、服务器软件 SQL Server/BizTalk Server/Commerce Server、开发工具软件 Visual FoxPro/Visual Basic 等多个产品中存在的 11 处安全漏洞。其中，4 项更新的综合评级为“严重”，修复了 8 个未公开的远程代码执行漏洞，其余 2 项更新的评级为“重要”。本月的更新修复了 5 个 IE 浏览器存在的漏洞。当中最严重的漏洞可导致用户使用 Internet Explorer 查看特定构造的恶意网页时远程执行代码。利用这些漏洞攻击者可以获得与当前用户相同的用户权限。

CNVD 收录的相关漏洞包括：Microsoft Windows 代码验证签名校验远程代码执行漏洞、Microsoft Windows Common Controls ActiveX 控件远程代码执行漏洞、Microsoft .NET Framework 参数验证远程代码执行漏洞、Microsoft Internet Explorer 打印特性远程代码执行漏洞（CNVD-2012-11158）、Microsoft Internet Explorer JScript9 远程代码执行漏洞（CNVD-2012-11160）、Microsoft Internet Explorer OnReadyStateChange 远程代码执行漏洞（CNVD-2012-11162）、Microsoft Internet Explorer SelectAll 远程代码执行漏洞（CNVD-2012-11164）、Microsoft Internet Explorer VML 样式远程代码执行漏洞（CNVD-2012-11166）等。上述漏洞的综合评级均为“高危”。CNVD 提醒广大 Microsoft 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/sites/main/preview/ldgg_preview.htm?tid=47080
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47078
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47060
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47075
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47077
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47081
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47096
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47079

2、Adobe 产品安全漏洞

Adobe Reader(也被称为 Acrobat Reader)是美国 Adobe 公司开发的一款 PDF 文件阅读软件。本周，上述 Adobe 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代码。CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 整数溢出漏洞（CNVD-2012-11145）、Adobe Acrobat/Reader 内存破坏漏洞（CNVD-2012-11146、CNVD-2012-11148）、Adobe Acrobat/Reader 安全绕过漏洞（CNVD-2012-11147）。目前，Adobe 已经发布这些漏洞的修补程序，CNVD 提醒相关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/sites/main/preview/ldgg_preview.htm?tid=47035
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47036
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47038

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47037

3、RealNetworks 产品安全漏洞

RealNetworks Helix Server 是一款支持多格式、跨平台的流媒体服务器软件。本周，RealNetworks Helix Server 被披露存在多个安全漏洞，攻击者可以利用漏洞构建恶意 URL，诱使用户解析，获得敏感信息，劫持用户会话，或发起拒绝服务攻击。CNVD 收录的相关漏洞包括：RealNetworks Helix Server 存在多个跨站脚本漏洞、RealNetworks Helix Server rn5auth 验证凭据解析远程代码执行漏洞、RealNetworks Helix Server 拒绝服务漏洞（CNVD-2012-11126、CNVD-2012-11127）、RealNetworks Helix Server 畸形 URL 栈耗尽漏洞、RealNetworks Helix Server 验证凭据信息泄露漏洞。其中，“RealNetworks Helix Server rn5auth 验证凭据解析远程代码执行漏洞”和“RealNetworks Helix Server 畸形 URL 栈耗尽漏洞”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 提醒相关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/sites/main/preview/ldgg_preview.htm?tid=46988

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46978

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46980

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46979

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46984

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46985

4、Siemens 网络设备产品安全漏洞

Siemens Scalance X Switches 是西门子公司开发的交换机设备；Siemens SCALANCE S 系列是用于保护以太网所有设备免受未经授权访问的安全模块。本周，上述产品被披露存在多个漏洞，攻击者可以利用漏洞进行暴力破解、拒绝服务攻击。CNVD 收录的相关漏洞包括：Siemens Scalance Firewall 暴力破解漏洞、Siemens Scalance Firewall 拒绝服务漏洞、Siemens Scalance X Switches HTTP 请求处理拒绝服务漏洞。其中，“Siemens Scalance Firewall 暴力破解漏洞”和“Siemens Scalance X Switches HTTP 请求处理拒绝服务漏洞”的综合评级为“高危”。目前，厂商已经发布其余漏洞的修补程序，CNVD 提醒相关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/sites/main/preview/ldgg_preview.htm?tid=46936

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46937

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46939

5、NetOp 远程控制客户端缓冲区溢出漏洞

NetOp Remote Control Client 是一款远程桌面控制软件。本周，上述产品被披露存在一个缓冲区溢出漏洞。应用程序处理较长的字符串会诱发异常，导致缓冲区溢出。攻击者可通过欺骗用户打开含有特定构造的文件，进而以用户权限执行任意代码。主要影响 NetOp Remote Control Client 9.5 版本。厂商尚未发布上述漏洞的修补程序，CN

VD 提醒广大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/sites/main/preview/ldgg_preview.htm?tid=46915

更多高危漏洞如表 3 所示, 详细信息可根据 CNVD 编号, 在 CNVD 官网进行查询。

参考链接: <http://www.cnvd.org.cn/publish/main/52/index.html>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2012-11208	PROMOTIC 内存错误引用远程代码执行漏洞	高	供应商发布了安全公告及相关补丁信息, 修复了此漏洞, 建议用户下载使用。避免攻击者构建恶意文件, 诱使用户解析可以应用程序上下文执行任意代码: http://www.promotic.eu/en/pmdoc/News.htm#ver801057
CNVD-2012-11205	nginx 'ngx_http_mp4_module.c'缓冲区溢出漏洞	高	供应商发布了安全公告及相关补丁信息, 修复了此漏洞, 建议用户下载使用。避免攻击者可以利用漏洞以用户上下文执行任意代码: http://nginx.org/download/patch.2012.mp4.txt
CNVD-2012-11201	Minerva Infotech CMS 'ID'参数 SQL 注入漏洞	高	暂无
CNVD-2012-11189	dev-GameSite 'id' SQL 注入漏洞	高	暂无
CNVD-2012-11152	Links 内存破坏漏洞 (CNVD-2012-11152)	高	供应商发布了安全公告及相关补丁信息, 修复了此漏洞, 建议用户下载使用。避免攻击者可以利用漏洞导致越界写: http://links.twibright.com/download/ChangeLog
CNVD-2012-11141	GE Energy D20/D200 Substation Controller 远程缓冲区溢出漏洞	高	暂无
CNVD-2012-11108	Novell iManager jclient 'EnteredAttrName'缓冲区溢出漏洞	高	供应商发布了安全公告及相关补丁信息, 修复了此漏洞, 建议用户下载使用。避免攻击者可以利用漏洞进行拒绝服务攻击或可以应用程序上下文执行任意代码: http://www.novell.com/support/viewContent.do?externalId=7002971
CNVD-2012-11130	CitrusDB SQL 注入漏洞	高	暂无

CNVD-2012-1111	Joomla!组件 VirtueMart 'virtuemart_userinfo_id' SQL 注入漏洞	高	暂无
CNVD-2012-11125	RealNetworks Helix Server rn5auth 验证凭据解析远程代码执行漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免可以以应用程序上下文执行任意代码： http://www.realnetworks.com/products-services/helix-server-proxy.aspx

表 3 部分高危漏洞列表

小结：4月10日，微软发布了2012年4月份的月度例行安全公告，共包含6项安全更新，修复了涉及Windows操作系统、.NET Framework、Office软件套件、Internet Explorer 浏览器、Forefront UAG、服务器软件 SQL Server/BizTalk Server/Commerce Server、开发工具软件 Visual FoxPro/Visual Basic 等多个产品中存在的11处安全漏洞。其中，4项更新的综合评级为“严重”，修复了8个未公开的远程代码执行漏洞，其余2项更新的评级为“重要”。

本周，Adobe 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代码。Siemens 和 RealNetworks 的产品也被披露存在多个综合评级为“高危”的漏洞，攻击者可以利用漏洞获取敏感信息，发起拒绝服务攻击；而 NetOp 远程桌面控制软件则被披露存在零日漏洞。上述软件在桌面终端用户以及企业用户中应用较多，需引起注意，加强防范。

本周重要漏洞修补信息

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 ProCurve 5400 zl Switch 安全漏洞

本周，HP 发布升级程序，修补了 ProCurve 5400 zl Switch 存在的安全漏洞。HP ProCurve 5400 zl Switch 是一款惠普公司开发的网络交换机。由于部分交换机分发的闪存卡存在恶意软件，如果用户连接浏览闪存卡可感染用户系统。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/sites/main/preview/bdgg_preview.htm?tid=15733

本周要闻速递

1. ThinkPHP 框架爆致命漏洞

日前乌云漏洞报告平台爆料称，ThinkPHP 框架存在“URL 取值任意代码执行”漏洞，黑客可借此在网站上执行任意 PHP 代码，甚至获取服务器管理员权限，同在此服

务器上的其他网站也可能受到牵连。ThinkPHP 是一款开源 PHP 框架，应用者遍及电子商务、教育培训、金融、政府等多个领域，包括大型门户网站游戏论坛、著名服装品牌网上商城等，都使用该 PHP 框架搭建。尽管此前 ThinkPHP 官方已发布修复漏洞的补丁，却未引起网站管理者的普遍重视，至今仍有大批网站因此存在被黑风险。

参考链接：<http://pcedu.pconline.com.cn/softnews/bingdu/1204/2751265.html>

2. 甲骨文下周二将发布 88 个补丁修复数据库漏洞

据甲骨文网站周四发布的提前通知显示，甲骨文下周二将发布 88 个安全补丁，修复产品中的安全漏洞。在甲骨文即将发布的补丁中，有 6 个补丁修复甲骨文数据库的安全漏洞，另外有 11 个补丁修复甲骨文 Fusion 中间件软件中的安全漏洞，其它安全漏洞影响的产品包括 BI Publisher 和 JDeveloper。甲骨文发布的安全补丁还包括：6 个修复甲骨文企业管理器网格控制产品漏洞的补丁；4 个补丁修复电子商务套装软件 ERP 应用中的漏洞；5 个补丁修复甲骨文供应链套装软件中的漏洞；15 个补丁修复各种仁科企业应用程序中的漏洞；17 个补丁修复甲骨文财务服务软件中的漏洞；2 个补丁修复甲骨文行业应用软件中的漏洞，1 个补丁修复甲骨文 Primavera 产品中的漏洞。另外 15 个补丁修复甲骨文 Sun 产品的漏洞，包括 GlassFish 应用服务器和 Solaris OS 操作系统中的安全漏洞。甲骨文还计划发布 6 个补丁修复 MySQL 数据库的安全漏洞。

参考链接：http://news.ccidnet.com/art/11099/20120413/3769535_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