

信息安全漏洞周报

2011 年 4 月 18 日-2011 年 4 月 24 日

2011 年第 16 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 118 个，其中高危漏洞 19 个、中危漏洞 79 个、低危漏洞 20 个。上述漏洞中，可利用来实施远程攻击的漏洞有 96 个。网上已经出现针对“Gesyttec GmbH ElonFmt ActiveX 'GetItem1()' 方法缓冲区溢出漏洞”、“SimplyPlay '.pls'文件远程缓冲区溢出漏洞”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 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。

成员单位上报漏洞统计

本周，共有 3 家成员单位报送了本周收录的全部 118 个漏洞，各单位报送情况如表 1 所示。其中，启明星辰报送数量较多。

成员单位	漏洞上报总数	私有漏洞数量
启明星辰	114	0
绿盟科技	10	0
恒安嘉新	9	0
总计	118（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、HP、Best Practical Solutions、Linux、Computer Associates、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	53	44.9%
2	HP	9	7.6%

3	Best Practical Solutions	6	5.1%
4	Linux	4	3.4%
5	Computer Associates	3	2.5%
6	Wireshark	3	2.5%
7	WebKit Open Source Project	3	2.5%
8	IBM	2	1.7%
9	Red Hat	2	1.7%
10	其他	33	28.1%

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、Oracle 发布安全公告，修复多个产品安全漏洞

本周，Oracle 发布了 2011 年 4 月份的安全更新。本次发布的安全更新修复了 Oracle Database、Fusion Middleware、Oracle Supply Chain、PeopleSoft、JD Edwards、Siebel、Health Sciences Applications 和 Sun 产品套件等存在的多个安全漏洞。攻击者可以利用这些漏洞发起拒绝服务、执行任意代码等攻击，获取敏感信息或操作部分数据。CNVD 收录的 Oracle 漏洞包括：Oracle Sun GlassFish/Java System 应用服务器远程验证绕过漏洞、Oracle Health Sciences Applications InForm 存在未明漏洞（CVE-2011-0800）、Oracle Siebel Globalization - Automotive 组件存在未明漏洞（CVE-2011-0843）、Oracle Siebel UIF 客户端组件存在未明漏洞（CVE-2011-0833）、Oracle PeopleSoft Enterprise 存在未明漏洞（CVE-2011-0828）、Oracle Health Sciences Applications InForm 存在安全漏洞、Oracle Application Service Level Management 组件存在漏洞（CVE-2011-0787）、Oracle 帮助组件存在漏洞（CVE-2011-0785）。其中，“Oracle Sun GlassFish/Java System 应用服务器远程验证绕过漏洞”的综合评级为“高危”。CNVD 提醒广大 Oracle 用户及时下载补丁程序进行修补。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05095>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05155>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05152>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05150>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05148>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05134>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05133>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05132>

2、HP 产品安全漏洞

本周，HP 的产品出现了多个安全漏洞，远程攻击者可以利用漏洞以管理员权限执行恶意操作、控制应用系统或窃取敏感信息。这些漏洞主要影响 HP Performance Insight、Insight Control、Systems Insight Manager、System Management Homepage、Network Node Manager i 等产品。CNVD 收录的相关漏洞包括：HP Performance Insight 未明信息泄露漏洞、HP Insight Control 存在未明漏洞（CVE-2011-1545）、HP Insight Control 存在未明漏洞（CVE-2011-1544）、HP Systems Insight Manager（CVE-2011-1542）未明跨站脚本漏洞、HP System Management Homepage（CVE-2011-1540）远程代码执行漏洞、HP System Management Homepage（CVE-2011-1541）远程未授权访问漏洞、HP Network Node Manager i 未明本地安全绕过漏洞。其中，“HP System Management Homepage（CVE-2011-1540）远程代码执行漏洞、HP System Management Homepage（CVE-2011-1541）远程未授权访问漏洞、HP Network Node Manager i 未明本地安全绕过漏洞”的综合评级均为“高危”。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-2011-05174>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05173>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05172>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05110>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05109>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05108>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05093>

3、WebKit 远程代码执行漏洞

WebKit 是一款开源的浏览器引擎。本周，WebKit 出现了多个远程代码执行漏洞。攻击者可以利用漏洞在受影响的程序中执行任意代码。CNVD 收录的相关漏洞包括：WebKit 未定义 DOM 原型附件远程代码执行漏洞、WebKit 分离(Detached)Body 元素远程代码执行漏洞、WebKit 畸形 SVG 文档处理远程代码执行漏洞。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了补丁程序，CNVD 提醒广大用户及时下载修复。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05100>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05099>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05098>

4、Avaya 产品安全漏洞

Avaya one-X Communicator 主要提供语音通信、桌面视频、可视语音留言、在线状态信息、电子邮件、即时消息处理、会议合并、通讯录管理以及通信记录管理等与终端通信、会议管理相关的应用；Avaya CS1000 Communications Server 是一款客户服务与协议应用

解决方案。本周，Avaya 的产品 one-X Communicator 和 Communication Server 出现安全漏洞。CNVD 收录的相关漏洞包括：Avaya one-X Communicator ActiveX 控件缓冲区溢出漏洞、Avaya CS1000 Communications Server 远程拒绝服务漏洞。攻击者可以利用漏洞发起拒绝服务攻击或在受影响的程序中执行任意代码。目前，厂商已经发布了补丁程序，CNVD 提醒广大用户及时下载修复。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05167>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05105>

5、Gesyttec GmbH ElonFmt ActiveX 'GetItem1()'方法缓冲区溢出漏洞

Gesyttec GmbH 是一款用于网络监测和分析的应用软件。本周，其 ElonFmt ActiveX 控件存在一个缓冲区溢出漏洞。攻击者通过构建内嵌恶意代码的网站页面，诱使用户访问，可以在受影响的用户主机上执行任意代码。目前，互联网上已经出现针对这个漏洞的攻击代码，主要影响 Gesyttec GmbH ElonFmt ActiveX 1.1.14 版本。厂商尚未发布这个漏洞的补丁，CNVD 建议用户及时关注厂商主页，以获取补丁程序或最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05171>

小结：本周，Oracle 发布安全公告，修复了包含 Oracle Database、Fusion Middleware、Oracle Supply Chain、PeopleSoft、JD Edwards、Siebel、Health Sciences Applications 和 Sun 产品套件在内的多个产品存在的安全漏洞。攻击者可以利用这些漏洞发起拒绝服务、执行任意代码等攻击，获取敏感信息或取得数据的管理操作权限，对广大 Oracle 用户构成较为严重的威胁。此外，HP、Avaya 产品和 WebKit 浏览器引擎均出现了多个综合评级为“高危”的安全漏洞。Gesyttec GmbH ElonFmt ActiveX 控件模块存在一个缓冲区漏洞，其攻击代码已在互联网上公开，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 多个安全漏洞

本周，Linux 发布升级程序，修补了 Linux Kernel（内核）存在的多个安全漏洞。攻击者利用漏洞可以发起拒绝服务攻击或提升特权。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/3496>
<http://www.cnvd.org.cn/patch/3481>
<http://www.cnvd.org.cn/patch/3482>



本周要闻速递

1.黑客假扮“猎头”利用 Flash “天窗”漏洞

近日，互联网上已出现多起黑客假扮“猎头”的事件，办公族对此应特别警惕。据悉，木马之所以能够“寄生”在 Excel 表格中，原因是人们常用的 Flash 出现了一个“天窗”高危漏洞，而 Excel、Word、PPT 等各种文档都可以嵌入 Flash 文件，这就意味着表格文档也可以成为木马的载体。此前，国际知名 IT 厂商 EMC 公司刚刚因此中招。该公司旗下安全部门 RSA 拥有著名的软硬件安全令牌产品，但是其公司内部网络却因为受到 Flash 漏洞攻击而被黑客入侵。根据 RSA 高级管理人员的博客透露，木马传播的途径正是一个名为“2011 年招聘计划”的 Excel 表格。与导致 RSA 受到攻击的 Flash 漏洞相比，最新的 Flash “天窗”漏洞威胁程度更高。安全专家介绍说，Flash “天窗”漏洞有两个特点：第一是影响范围广，Windows、Android、MacOS 等各种操作系统的用户都存在风险；第二是攻击花样多，网页游戏、视频、文档等所有可以运行 Flash 的载体都可能成为木马通道。安全专家建议，在 Adobe 公司修复 Flash “天窗”漏洞之前，网民不可随意打开来历不明的文件和网址链接，并要为电脑安装有效安全软件，可以保护重要资料不被木马窃取。

参考链接：<http://www.hackbase.com/news/2011-04-22/59872.html>

2.微软披露谷歌安全漏洞

4 月 22 日消息，据国外媒体报道，微软放弃了不披露非微软产品漏洞的原则，出具了两份针对谷歌公司产品的安全报告。相对来说，谷歌披露微软公司的软件漏洞的次数就比较多。这两份安全报告所涉及的产品均为 Chrome 浏览器。尽管谷歌在该浏览器中采用了沙箱等一系列安全防护技术，其安全水平已经高于 IE，但微软仍然让网络用户知晓，Chrome 也有其弱点。同时微软声明在公开漏洞之前已经与谷歌沟通，因此在微软披露时，该漏洞已经得到修复。其中一个漏洞是 HTML5 在 Chrome 中执行时会导致信息泄露，另一个漏洞是允许沙箱远程代码执行。但是两个漏洞都有一定的局限性，一个漏洞要求攻击者拥有包含私人信息的网络资源 IP 地址，另一个漏洞则要求代码必须在沙箱内运行，才能攻击成功。

参考链接：http://news.ccidnet.com/art/11099/20110422/2370397_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