

### 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)本周共收集和整理信息安全漏洞 45 个,其中高危漏洞 7 个、中危漏洞 10 个、低危漏洞 28 个。上述漏洞中,可利用来实施远程攻击的漏洞有 35 个。经检测发现,网上已经出现针对“华为 EchoLife HG520c AutoRestart.html 页面远程拒绝服务漏洞”、“Microsoft IE 8 跨站脚本过滤漏洞”的零日攻击代码,请广大用户注意做好防护措施。目前,相关厂商已经为 21 个漏洞提供了修补方案,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 IE 8 跨站脚本过滤漏洞

Microsoft Internet Explorer 8 包含的 XSS 过滤器在处理特殊构建的 SCRIPT 标签时存在漏洞,远程攻击者可以利用漏洞对原来没有 XSS 跨站脚本漏洞的站点构建跨站脚本攻击。IE8 中引入了新的跨站脚本防范机制,其基本原理是在浏览器中创建过滤器以检测和防范某些类型的恶意跨站脚本攻击。具体来讲,当过滤器完成上述匹配时就会修改某些字符串,这样攻击就无法执行。例如,如果在出站请求的 GET 参数和响应体中都检测到了 `<script>alert(0)</script>` 字符串,就会触发中和机制,将该字符串更改为 `<sc#ipt>alert(0)</script>`,这样所注入的脚本就无法执行。但是,浏览器在呈现之前更改服务器的响应可能会产生非预期的结果,攻击者可以滥用中和机制阻断页面中的无害内容。目前,厂商尚未发布补丁或升级程序,建议用户随时关注厂商主页以获取最新版本。

参考链接:

<http://blogs.technet.com/msrc/archive/2010/04/19/guidance-on-internet-explorer-xss-filter.aspx>

#### 2、华为 EchoLife HG520 存在两个远程拒绝服务漏洞

华为 EchoLife HG520 是专为家庭上网和家庭办公设计的家庭网关产品系列。该系列产品存在的两个漏洞是: 华为 EchoLife HG520c AutoRestart.html 页面远程拒绝服务漏洞,远程用户可以通过向该页面提交恶意的 GET 请求导致设备重启; 华为 EchoLife HG520c

rpLocalDeviceJump.html页面远程拒绝服务漏洞，远程用户向EchoLife HG520的/rpLocalDeviceJump.html页面提交了长度超过7个字符的index变量的话，就会导致设备重启。目前，厂商尚未发布补丁或升级程序，建议用户随时关注厂商主页以获取最新版本。  
参考链接：<http://www.exploit-db.com/exploits/12297>

### 3、Google Chrome存在多个安全漏洞

Google Chrome是一款开源的WEB浏览器。Google Chrome 4.1.249.1059之前版本存在多个安全漏洞，漏洞可用于实施跨站脚本攻击、内存破坏、特权提升等恶意活动。具体漏洞信息为：chrome://net-internals存在跨站脚本攻击风险、chrome://downloads存在跨站脚本攻击风险、V8 bindings存在内存破坏问题、表单存在类型混淆错误、通过开发工具可引用本地文件、可能以新标签页的特权装载页面。目前，Google Chrome 4.1.249.1059已经修复以上漏洞，建议用户下载使用。

参考链接：<http://www.google.com/chrome>

### 4、VLC Media Player 存在多个安全漏洞

VLC Media Player是一款流行的多媒体播放程序。VLC Media Player存在多个安全漏洞，远程攻击者通过利用该漏洞可以应用程序权限执行任意指令。具体漏洞信息为：A/52音频解码器存在错误可触发基于堆的缓冲区溢出、DTS音频解码器存在错误可触发基于堆的缓冲区溢出、MPEG音频解码器存在错误可触发基于堆的缓冲区溢出、AVI分路器存在错误可触发非法内存访问、ASF分路器存在错误可触发非法内存访问、Matroska分路器存在错误可触发非法内存访问、处理XSPF播放列表存在错误可触发非法内存访问、ZIP实现存在错误可触发非法内存访问、RTMP实现存在错误可触发基于堆的缓冲区溢出。目前，VLC media player 1.0.6已经修复此漏洞，建议用户下载使用。

参考链接：<http://download.videolan.org/pub/videolan/vlc/1.0.6/vlc-1.0.6.tar.bz2>

### 5、HP Operations Manager 缓冲区溢出漏洞

HP OpenView Operations是一款分布式客户机/服务器软件，用于管理分布式环境。HP OpenView Operations SourceView ActiveX控件(srcvw32.dll或srcvw4.dll)存在边界错误，提交超长参数给"LoadFile()"方法，可触发基于栈的缓冲区溢出。目前，用户可参考如下供应商提供的安全公告获得补丁程序。

参考链接：

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02078800>

**小结：**本周 CNVD 所整理的漏洞信息中，IE8、EchoLife HG520 网关、Google Chrome 浏览器、VLC Media Player、HP Operations Manager 等均出现了严重漏洞。这些漏洞严重影响我国网民的用网安全，请广大用户注意采取安全防范措施，尽快下载相关补丁程序。

## 本周重要漏洞修补信息

本周，CNVD 整理和发布以下重要的漏洞修补信息。

## 1、Apache 安全公告

Apache 于 4 月 21 日发布了一个安全公告以及相应补丁，修复了 Apache Tomcat 校验头 Realm 名信息泄漏漏洞。建议用户尽快下载使用，避免远程攻击者利用漏洞以应用程序权限执行任意代码。

补丁下载链接：<http://svn.apache.org/viewvc?view=revision&revision=936541>

## 2、Cisco 重要安全公告

Cisco 于 4 月 21 日发布重要安全公告（cisco-sa-20100421-vsc），修复了 Cisco 小型商业视频监控摄像机和 4 端口路由器验证绕过漏洞。建议用户尽快下载使用，以避免受到漏洞的影响。

补丁下载链接：<http://www.cisco.com/warp/public/707/cisco-sa-20100421-vsc.shtml#@ID\>

## 本周要闻速递

### 1、微软将在六月份再次修复 IE8 跨站漏洞

微软计划在 6 月份更新 IE 8 浏览器以阻止利用 IE8 浏览器中的跨站脚本过滤器对网站实施攻击。研究人员 Eduardo Vela Nava 和 David Lindsay 在黑帽会议上演示了黑客如何利用 IE 8 的跨站脚本过滤器对本来应该有免疫能力的网站实施的攻击。这个演示促使微软决定更新 IE 8。研究人员称，容易受到这种攻击的网站包括微软自己的必应搜索引擎、Digg、谷歌、Twitter、维基百科等许多网站。

参考链接：<http://www.hackbase.com/news/2010-04-21/34830.html>

### 2、微软 Windows MS10-025 补丁没有用被撤回

微软今天撤下了上周针对 Windows 2000 Server 的安全补丁 MS10-025，原因是微软表示该补丁未能解决实质性问题。MS10-025 是用来修复 Windows 2000 Server 中 Windows Media Services 中出现的一个漏洞，但是它并没有解决任何问题。微软表示截至目前还没有发现利用该漏洞进行的攻击行为。下周，微软将发布一个新的补丁，解决 MS10-025 本应解决的问题。

参考链接：<http://www.cert.org.cn/articles/news/common/2010042324949.shtml>

### 3、McAfee 5958 病毒更新程序故障令全球各大企业用户电脑哑火

McAfee 杀毒软件通过企业用更新服务器更新新版 5958 病毒库后，软件会将 Windows XP 操作系统中的重要系统文件 svchost.exe 强行删除，删除这个文件的结果则是导致杀毒软件和系统出现许多异常故障，如频繁重启以及无法进行网络连接等等。尽管针对这个故障目前已经有了一些解决方案，但是这种解决方案出台的时间为时已晚，预计 McAfee 软件的这次故障已经影响到了全球数百万台电脑，据传 Intel 公司内部所用电脑甚至 Dish Network 公司的数据中心也已经受到了此故障的影响。据 McAfee 表示，他们已经将 5958 版更新从企业更新服务器上撤掉，而且普通用户也不会受到这次更新的影响。

参考链接：<http://cnbeta.com/articles/109251.htm>

## 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](http://www.cert.org.cn)

邮箱：[vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话：010-82990999