

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高。

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 126 个，其中高危漏洞 45 个、中危漏洞 45 个、低危漏洞 36 个。上述漏洞中，可利用来实施远程攻击的漏洞有 114 个。本周，Linux 曝出本地提权 0-day 漏洞，CNVD 提醒相关用户做好防范措施。本周收录的安全漏洞中，已有 117 个漏洞由相关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、TLS/SSH 协议漏洞致使多款产品存在安全漏洞

传输层安全协议/安全套接层协议(TLS/SSH)是确保互联网上通信应用和其用户隐私的协议。多个厂商的TLS/SSH协议实现中的会话重新协商过程面临中间人攻击的威胁，扮演为中间人的恶意服务器可以向应用协议流的开始处注入受控的明文，进而实施网络欺骗，攻击者可绕过某些安全限制、操作部分数据、获得敏感信息、对服务进行拒绝服务攻击或完全控制受影响系统。漏洞涉及Sun Java、Oracle、IBM等著名厂商的多款产品。CNVD本周收录的与该协议漏洞相关的漏洞包括：IBM WebSphere Application Server for z/OS存在多个安全漏洞、Oracle JRockit存在多个未明漏洞、多个厂商TLS协议会话重新协商中间人攻击漏洞、IBM DB2数据操作和缓冲区溢出漏洞、Oracle WebLogic Server TLS协议存在漏洞、Oracle Supply Chain产品"Transportation Management"组件存在未明错误漏洞、Sun Java JSSE TLS/SSL组件存在未明错误漏洞。相关厂商已为上述漏洞提供了修补程序，CNVD提醒广大用户及时下载更新，避免安全漏洞引发的网络攻击事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-00746>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01390>
<http://www.cnvd.org.cn/vulnerability/CNVD-2009-14046>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-00732>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01400>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02344>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02537>

2、GNU Linux存在本地提权漏洞

Linux 是一款开放源代码的操作系统。本周，CNVD 成员单位上报了 2 个 Linux 操作系统的本地提权高危漏洞：GNU glibc 动态链接器'SORIGIN'本地特权提升漏洞、Linux 内核可靠数据报套接字(RDS)协议本地特权提升漏洞。

攻击者利用 GNU glibc 动态链接器'SORIGIN'本地特权提升漏洞可以在取得普通用户权限的情况下（具备创建、执行文件权限），即可提升至根用户（root）权限，实现对操作系统主机的完全控制。CNVD 对该漏洞及相关攻击程序进行了分析，攻击时主要是利用 gcc 编译器 glibc 库中忽略某变量路径的缺陷，通过控制变量路径欺骗执行自定义的 DSO(动态共享对象：Dynamic Share Object)代码实现攻击。CNVD 对该漏洞进行了初步验证，目前已知的受影响系统范围包括：Fedora Core 13 系列、RedHat 系列、CentOS5 系列。由于 Linux 相关函数库的通用性，不排除其他系统也可被利用的情况。目前相关厂商尚未提供解决方案和措施，CNVD 提醒广大 Linux 用户提高警惕，加强防范，要注意检查 Linux 主机上普通用户的安全管理是否存在薄弱点，并对用户安全日志进行审计。

对于 Linux 内核可靠数据报套接字(RDS)协议本地特权提升漏洞，Linux 上的 recvmsg()样式套接字调用都是使用 iovec 结构，允许用户指定基地址和用于接收套接字数据的缓冲区大小。每个报文的协议族负责定义拷贝套接字的函数，由内核接收并返回给用户空间允许用户程序处理接收到的网络数据。当执行拷贝数据到用户空间的操作时，RDS 协议在使用 copy_to_user_inatomic()函数之前没有验证用户提供的 iovec 结构指向的合法用户控件地址的基地址，导致可提供一个内核地址作为 iovec 基地址，提交 recvmsg()样式套接字调用后，本地用户可写任意数据到内核内存，从而提升特权，如 root。Linux kernel 2.6 所有版本均受该漏洞的影响。针对该漏洞，厂商已发布了安全公告及相关补丁信息，建议用户尽快下载使用，避免本地攻击者利用漏洞提升权限。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02541>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02483>

3、Sun Solaris 多个版本存在安全漏洞

Sun Solaris 是一款商业性质的 UNIX 操作系统。Sun Solaris 存在多个安全漏洞，允许恶意用户获得敏感信息、提升特权或进行拒绝服务攻击。CNVD 本周收录的 Sun Solaris 漏洞包括："Live Upgrade"组件存在未明错误、"Scheduler"组件存在未明错误、"Device Drivers"组件存在未明错误、"Kernel/Disk Driver"组件存在未明错误、"USB"组件存在未明错误、"SCSI enclosure services device driver"组件存在未明错误。目前厂商已发布这些漏洞的修补程序，CNVD 提醒广大用户及时下载更新，避免此类漏洞引发的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02052>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02465>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02464>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02462>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02460>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02459>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02457>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02414>

4、HP Systems Insight Manager存在两未明高危漏洞

HP Systems Insight Manager是一款实现对服务器、存储、网络等IT基础设施进行统一管理的解决方案。HP Systems Insight Manager存在未明输入验证错误，允许攻击者进行跨站脚本攻击，可获得用户敏感信息或劫持目标用户会话。此外HP Systems Insight Manager还存在未明错误，允许验证用户提升特权。影响的产品包括HP Systems Insight Manager 6.1及其之前的版本，目前供应商已修复上述漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02485>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02486>

5、Windows Server 2008 存在颜色控制面板 DLL 装载任意代码执行漏洞

Windows Server 2008是一款微软发行的服务器操作系统。颜色控制面板应用程序(colorcpl.exe)使用的颜色控制面板库(colorui.dll)以不安全的方法装载库，如sti.dll。攻击者诱使用户打开位于远程WEBDAV或SMB共享上的CAMP、CDMP、GMMP或者ICC Profile(.icm和.icc)文件，可装载任意库，导致任意代码执行。目前相关厂商尚未提供解决方案和措施，CNVD提醒广大用户提高警惕，加强防范措施。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02433>

小结：本周，Linux 出现了 2 个本地提权 0-day 漏洞，其中 Linux 内核可靠数据报套接字(RDS)协议本地特权提升漏洞已经发布修补程序，请广大 Linux 用户及时下载更新；目前，GNU glibc 动态链接器'\$ORIGIN'本地特权提升漏洞尚未发布修补程序，请广大 Linux 用户提高警惕，加强防范，注意检查 Linux 主机上普通用户的安全管理是否存在薄弱点。此外，Sun Java、Oracle、IBM、Sun Solaris、Windows Server 2008、HP Systems Insight Manager等均出现安全漏洞。这些漏洞对用户的信息安全和公共互联网网络安全构成威胁，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、Sun Java 发布多个产品或组件的更新补丁程序

Java 是由 Sun Microsystems 公司推出的 Java 程序设计语言和 Java 平台的总称。本周，CNVD 收录了多个 Sun Java 相关产品或组件的多个漏洞的补丁更新程序。涉及的重要的补丁包括：Sun Java 可诱使序列化 API 的 defaultReadObject 方法多次设置漏洞的补丁、Sun Java 中 JDK Deployment Toolkit 工具存在安全漏洞的补丁、Sun Java JDK 2D 组件存在

安全漏洞的补丁、Sun Java 对象反序列化存在竞争条件漏洞的补丁、Sun Java OpenJDK ICU Opentype 布局引擎漏洞的补丁、Sun Java OpenJDK ICC profile 远程代码执行漏洞的补丁、Sun Java 中 JDK sound 组件存在安全漏洞的补丁等，CNVD 提醒相关用户及时下载补丁更新。

补丁下载链接：<http://www.cnvd.org.cn/patch/1435>

<http://www.cnvd.org.cn/patch/1431>

<http://www.cnvd.org.cn/patch/1432>

<http://www.cnvd.org.cn/patch/1433>

<http://www.cnvd.org.cn/patch/1428>

<http://www.cnvd.org.cn/patch/1429>

<http://www.cnvd.org.cn/patch/1430>

2、IBM Informix Dynamic Server 发布补丁更新程序修复多个重要安全漏洞

IBM Informix Dynamic Server 是一款数据库服务程序。本周 CNVD 收录的相关漏洞补丁包括：IBM Informix Dynamic Server oninit.exe 服务远程栈溢出漏洞的补丁、IBM Informix Dynamic Server librpc.dll 库整数溢出漏洞的补丁、IBM Informix Dynamic Server DBINFO 关键字远程栈溢出漏洞的补丁、IBM Informix Dynamic Server 'oninit.exe'缓冲区溢出漏洞的补丁、IBM Informix Dynamic Server 'oninit.exe'缓冲区溢出漏洞的补丁、IBM Informix Dynamic Server DBINFO 关键词远程栈缓冲区溢出漏洞的补丁。CNVD 提醒广大用户及时下载更新升级程序，避免网络攻击事件发生。

补丁下载链接：<http://www.cnvd.org.cn/patch/1334>

<http://www.cnvd.org.cn/patch/1335>

<http://www.cnvd.org.cn/patch/1336>

<http://www.cnvd.org.cn/patch/1437>

<http://www.cnvd.org.cn/patch/1440>

<http://www.cnvd.org.cn/patch/1442>

本周要闻速递

1、iPhone 4 再现漏洞：短信删掉还能再现

据报道，最近 iPhone 4 又被用户们发现一重大漏洞，短信删除后，用 spotlight 搜索时还能再找回来，这样的漏洞严重威胁到了用户的隐私安全。媒体记者根据网友的反应，对 iPhone 4 进行了测试，结果证实了上述漏洞。不过，随着记者的进一步测试发现，这一短信“复活”现象并不是所有的机型都会出现，只是出现在了部分机型中。提醒已在使用 iPhone 4 的用户及时检验自己的手机是否也会出现短信“死而复生”的现象，若测试的机型遇到同样的问题，可以尝试在设置通用界面上，删除短信搜索功能，来避免发生短信复活现象。如果仍不能解决此问题，建议您找苹果厂商解决，避免隐私泄漏。

参考链接：<http://tech.sina.com.cn/t/2010-10-20/16504768495.shtml>

2、谷歌发布 Chrome 浏览器安全补丁 修复多版本漏洞

据报道，谷歌对 Chrome 网络浏览器进行了安全更新，以免遭受攻击。谷歌 Chrome 浏览器此次升级修复了多个版本浏览器的十个漏洞。其中，有一个为重要级别的修复，防止黑客攻击 AutoFill 上的一个漏洞。专家建议用户和管理人员及时进行升级更新，以免使用受到影响。

参考链接：<http://news.hexun.com/2010-10-22/125223844.html>

3、OWASP2010 中国峰会于 2010 年 10 月 22 日在京召开

OWASP 是一个开源非盈利全球性安全组织，致力于应用软件的安全研究。2010 中国峰会于 10 月 22 日在北京新世纪日航酒店召开，会议以“大融合时代应用安全”为主题，希望通过本次会议能够更好推动应用安全技术在国内的发展。本届年会将围绕应用安全的相关领域，在“应用安全威胁”、“安全开发流程”、“代码安全”、“安全测试(渗透测试)”、“各行业应用安全需求及技术”等多个方面开设培训和演讲专题。

参考链接：<http://www.cww.net.cn/zhuanti/OWASP2010/>

4、Java 框架超越 Adobe 成为新科漏洞王

微软研究人员最近表示，Oracle 的 Java 框架已经超过之前的 Adobe 系列软件成为最受攻击者关注的应用。根据公布的 Microsoft 恶意软件保护中心的数据，到今年年度，Java 漏洞的数量超过了 Adobe，并开始承受每季度几百万次的攻击。一直以来，Adobe 的 Flash 播放器因为用户数量庞大而成为黑客的主战场，而 Java 作为一种在后台运行的无处不在的技术也开始受到关注。最普遍的攻击方法是在浏览器访问正常网站时利用被隐藏的 iFrame 或 JavaScript 重定向至一个带有恶意 Java 小程序的恶意网页。

参考链接：<http://www.cnbeta.com/articles/124851.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

邮箱：vreport@cert.org.cn

电话：010-82990999