

信息安全漏洞周报

2010 年 8 月 16 日-2010 年 8 月 22 日

2010 年第 32 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低。

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 28 个，其中高危漏洞 0 个、中危漏洞 4 个、低危漏洞 24 个。上述漏洞中，可利用来实施远程攻击的漏洞有 22 个。目前，有关厂商已针对 13 个漏洞提出了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。

本周重要的漏洞信息

本周，CNVD 整理和发布以下重要漏洞信息。

1、Apache CXF 存在 XML 文档类型声明处理漏洞

Apache CXF 是一个开源的服务框架，支持使用 JAX-WS、JAX-RS 等前端编程 API 来编译和开发服务。CXF 未正确限制、处理 XML 文档类型声明（DTD）。远程攻击者可通过提交恶意请求以读取本地文件内容，占用 CPU 和内存资源，实施拒绝服务攻击。目前 Apache 已经发布补丁程序修复上述安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01662>

2、Serv-U 存在安全绕过和拒绝服务漏洞

Serv-U 是一款 FTP 服务器软件。Serv-U 在处理虚拟路径时存在错误，操作者无需权限即可创建目录。另外，Serv-U 在处理某些 URL 参数时也存在错误，可导致 Serv-U 程序崩溃。攻击者可利用漏洞绕过安全限制、进行拒绝服务攻击。目前 Serv-U 发布的 10.2.0.0 版本已经修复上述漏洞，建议相关用户尽快下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01674>

3、Linux 内核存在用户空间栈增长漏洞

Linux 是一款开放源代码的操作系统。Linux 内核未正确限制用户空间中应用程序的栈增长，攻击者可通过构建恶意应用程序触发栈溢出，致使栈无提示地覆盖其他内存映射区域，最终导致权限提升。Linux Kernel 2.6.32.19、2.6.34.4 和 2.6.35.2 等版本已经修复上述漏洞，建议相关用户尽快下载使用。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01665>

小结: 本周, Apache、Serv-U、Linux 内核等产品曝出安全漏洞。这些漏洞可被攻击者利用于实施远程或本地攻击, 对国内相关用户的信息安全和公共互联网网络安全构成威胁, 请使用以上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 Kernel 文件内存泄漏导致本地信息泄漏的补丁

Linux 'net/sched/act_*.c'存在内存泄漏问题, 由于没有正确初始化 dumped 结构的所有字段, 可导致在 tc dump 中泄漏至少 32 位内核内存给用户空间, 最终导致敏感信息泄漏。目前厂商已经发布了升级补丁以修复这个安全问题, 建议相关用户尽快下载补丁程序修复漏洞。

补丁下载链接: <http://www.cnvd.org.cn/patch/834>

本周要闻速递

1、数个 Windows 应用程序被曝存在相同高危漏洞

8 月 23 日消息, 据外电报道, 大约有 40 种不同的 Windows 应用程序存在一种高危漏洞。该漏洞可以让攻击者劫持电脑并让它们感染恶意软件。研究人员建议用户关闭 SMB 139 和 445 端口, 禁用 WebDAV 服务来防止病毒在内部网络中传播。目前微软没有对这个消息做出任何官方表示。

参考链接: <http://www.hackbase.com/news/2010-08-23/37336.html>

2、英特尔宣布将以 76.8 亿美元收购 McAfee

北京时间 8 月 19 日晚间消息, 据国外媒体报道, 英特尔宣布将以每股 48 美元现金收购安全软件公司 McAfee, 此笔交易总值将达约 76.8 亿美元。该收购价格超过 McAfee 周三收盘价 29.93 美元的 60%。周四 McAfee 股价飙升 58%, 至 47.42 美元。英特尔与 McAfee 董事会均全票同意收购交易, 但交易仍需经过 McAfee 股东大会以及相关部门的批准。

参考链接: <http://tech.sina.com.cn/it/2010-08-19/20454565436.shtml>

3、谷歌修复 10 个 Chrome 安全漏洞 兑现 1 万美元奖金

据资讯网站 Computerworld 报道, 本周五, 谷歌修复了 Chrome 浏览器中的 10 个安全漏洞, 并为此支付 1 万美元奖金。据了解, 存在于 Chrome 5.0.375.125 的漏洞中有两个被标识为最高级别的“高危”, 另有七个属于“重要”, 只有一个是“普通”。部分漏洞会被感染恶意文件, 其中包括 SVG 图片文件和 MIME 格式文件; 还有部分漏洞会安装恶意工具, 窃取用户密码等重要信息。

参考链接: <http://www.hackbase.com/news/2010-08-23/37340.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