

信息安全漏洞周报

2010 年 11 月 8 日-2010 年 11 月 14 日

2010 年第 44 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 132 个，其中高危漏洞 24 个、中危漏洞 28 个、低危漏洞 80 个。上述漏洞中，可利用来实施远程攻击的漏洞有 116 个。经跟踪发现，网上已经出现针对“Linux Kernel ‘net/core/filter.c’ 本地信息泄漏漏洞”、“WordPress cformsII 插件 rs 和 rsargs 参数脚本注入漏洞”、“Apache Shiro 目录遍历漏洞”、“Free CD to MP3 Converter 缓冲区溢出漏洞”以及“MySQL ‘WITH ROLLUP’拒绝服务漏洞”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。本周收录的安全漏洞中，已有 106 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 多款产品存在安全漏洞

本周，微软产品 Office 和 Forefront 出现了多个安全漏洞，CNVD 收录的相关漏洞包括：Microsoft PowerPoint ‘PP7X32.DLL’ 堆缓冲区溢出漏洞、Microsoft PowerPoint 整数下溢导致堆损坏漏洞、Microsoft Office RTF 文件栈缓冲区溢出漏洞、Microsoft Office 解析超大 SPID 时存在远程代码执行漏洞、Microsoft Office Art 会话记录远程代码执行漏洞、Microsoft Office 绘图异常处理远程代码执行漏洞、Microsoft Forefront Unified Access Gateway ‘Signurl.asp’跨站脚本漏洞、Microsoft Forefront Unified Access Gateway Mobile Portal 跨站脚本漏洞、Microsoft Forefront Unified Access Gateway 伪造漏洞。攻击者利用这些漏洞可获取敏感信息、执行任意代码、获得管理员权限等。目前微软已经发布了用于修复这些漏洞的升级补丁，CNVD 提醒广大用户及时下载更新，避免引发此漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02842>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02841>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02840>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02839>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02838>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02837>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02836>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02835>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02834>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02831>

2、Linux 存在多个安全漏洞

Linux是一款开放源代码的操作系统。本周，Linux出现了多个安全漏洞，CNVD收录的Linux安全漏洞包括：Linux Kernel Block层拒绝服务漏洞、Linux Kernel ‘io_submit_one()’ 空指针应用拒绝服务漏洞、Linux Kernel Futex宏本地拒绝服务漏洞、Linux Kernel ‘net/core/filter.c’ 本地信息泄漏漏洞、Linux Kernel net/子系统多个本地信息泄露漏洞、Linux内核 ‘kvm/x86.c’ 本地信息泄漏漏洞、Linux Kernel KVM内存泄漏漏洞、Linux Kernel ‘x25_parse_facilities()’ 远程拒绝服务漏洞、Linux Kernel CAN协议信息泄漏漏洞、Linux Kernel ‘inet_diag.c’ Netlink消息拒绝服务漏洞等，这些漏洞会引发内存泄漏、敏感信息泄露、拒绝服务等威胁。其中，“Linux Kernel ‘net/core/filter.c’ 本地信息泄漏漏洞”为0-day漏洞，互联网上已经出现针对Linux Kernel 2.6.x版本的漏洞攻击程序。目前Linux官方已经修补了这些漏洞，CNVD建议用户及时下载更新补丁程序。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02848>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02833>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02821>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02819>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02770>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02757>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02756>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02755>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02754>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02752>

3、Adobe Flash Player存在多个高危安全漏洞

Adobe Flash Player 是一款被广泛使用的多媒体程序播放器。本周，Adobe Flash Player 出现多个高危安全漏洞。这些漏洞可导致用户应用程序崩溃，甚至可被利用入侵主机系统。CNVD 收录的重要安全漏洞包括：Adobe Flash Player 存在内存破坏漏洞、Adobe Flash Player 存在拒绝服务漏洞、Adobe Flash Player 存在信息泄漏漏洞(仅限 Macintosh 平台和 Safari 浏览器)、Adobe Flash Player 存在输入验证漏洞、Adobe Flash Player 存在内存破坏漏洞(仅限 ActiveX)等。目前，Adobe 已发布了这些漏洞的升级补丁，CNVD 提醒广大用户关注厂商发布的更新信息并及时下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02779>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02778>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02777>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02776>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02775>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02774>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02773>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02771>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02769>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02768>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02766>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02765>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02763>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02762>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02761>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02760>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02759>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02758>

4、ProFTPD 多个模块存在目录遍历和缓冲区安全漏洞

ProFTPD是一款开放源代码FTP服务程序。本周，ProFTPD的多个模块出现了目录遍历和缓冲区溢出漏洞。其中，ProFTPD的src/netio.c文件中的pr_netio_telnet_gets()函数在处理包含有Telnet IAC转义序列的用户输入时存在栈溢出。远程攻击者可以通过向FTP或FTPS服务提交恶意输入转而执行任意代码。此外，mod_site_misc模块中存在多个输入验证错误，攻击者可以通过目录遍历攻击写入或删除任意目录、更改文件时间。目前，厂商已经发布补丁更新程序，CNVD提醒广大用户下载更新，避免引发此漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02767>

5、Novell GroupWise产品存在安全漏洞

Novell GroupWise是一款跨平台协作软件。本周，该产品出现多个安全漏洞。CNVD本周收录的Novell GroupWise产品的重要安全漏洞有：Novell GroupWise Internet Agent组件Content-Type多个值解析栈溢出漏洞、Novell GroupWise Internet Agent TZNAME Parsing远程代码执行漏洞、Novell Groupwise Internet Agent IMAP LIST Command远程代码执行漏洞、Novell GroupWise Internet Agent Content-Type Parsing Integer Signedness远程代码执行漏洞、Novell GroupWise Internet Agent Content-Type String Parsing 远程代码执行漏洞等。攻击者会利用这些漏洞可实施远程执行代码攻击。目前，厂商已发布了升级补丁修复这些安全漏洞，CNVD建议用户关注厂商主页以获得修补方案。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02860>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02809>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02808>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02807>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02806>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02805>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02804>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02803>

6、Cisco 存在多个安全漏洞

Cisco Unified Intelligent Contact Management Enterprise是思科公司统一通信系统的一个重要组成部分。它提供了一套集成功能，使企业可部署一个混合了多个通信渠道的解决方案，并方便地从传统自动呼叫分发器 (ACD) 移植到基于IP的ACD。本周CNVD收录的该产品的漏洞包括：Cisco ICM Setup Manager Agent.exe HandleUpgradeTrace存在远程代码执行漏洞、Cisco ICM Setup Manager Agent.exe HandleUpgradeAll存在远程代码执行漏洞、Cisco ICM Setup Manager Agent.exe HandleQueryNodeInfoReq存在远程代码执行漏洞、Cisco ICM Setup Manager Agent.exe AgentUpgrade存在远程代码执行漏洞。攻击者可以利用这些漏洞可以以SYSTEM用户权限执行任意代码。目前，厂商已经发布补丁程序修复上述漏洞，CNVD提醒广大用户及时下载更新，避免引发此漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02802>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02801>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02800>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02799>

小结：本周，Adobe 发布了 APSB10-27 号安全公告，修补了运行在 WINDOWS 和 LINUX 操作系统下的 Adobe Flash Media Server 出现的三个安全漏洞。此外，微软、Linux、Cisco、Novell GroupWise 等应用广泛的产品均出现了多个安全漏洞，对国内用户的信息安全和互联网网络安全构成较为严重的威胁，请使用上述软件的相关机构和个人请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、IBM 发布了安全公告修补了多个漏洞

IBM OmniFind Enterprise Edition 是一款企业级的搜索引擎，IBM Tivoli 是一款目录服务器。本周，CNVD 收录了 IBM OmniFind Enterprise Edition 及 IBM Tivoli 出现的多个安全漏洞，远程攻击者可以利用这些漏洞导致应用程序崩溃或者注入任意脚本代码。其中有些漏洞还可以使本地攻击者获得 root 权限。目前，厂商已经发布了上述漏洞的修复升级程序，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/1674>

<http://www.cnvd.org.cn/patch/1677>

<http://www.cnvd.org.cn/patch/1678>

<http://www.cnvd.org.cn/patch/1691>



本周要闻速递

1、Adobe Flash Player 升级修复大量高危漏洞

Adobe 于 11 月 9 日对其 FlashPlayer 10.1 进行了一次集中升级,新版本号为 10.1.102.64,修复了大量高危级别的安全漏洞。此次升级主要针对 Windows、Mac、Linux、Solaris 系统的 Flash Player 10.1.85.3 或更早版本。此外,Android 手机平台的 Flash Player 10.1.95.1 同样受安全漏洞的影响。请使用 Adobe Flash Player 的用户及时下载补丁更新程序。

参考链接: http://security.zdnet.com.cn/security_zone/2010/1109/1934072.shtml

2、谷歌修复 Chrome 浏览器 12 个高危安全漏洞

11 月 8 日消息,谷歌上周修复了 Chrome 浏览器中的 12 个安全漏洞。所有这些安全漏洞都是谷歌安全团队列为高风险等级的安全漏洞。使用安全补丁的 Chrome 浏览器还包括一个为 Adobe 的 Flash 播放器提供的补丁,提前为谷歌用户提供了一个修复严重安全漏洞的补丁。黑客一直在使用非法的 PDF 文件利用这个安全漏洞实施攻击。Adobe 计划在本星期晚些时候为其它浏览器用户发布这个 Flash 补丁。Chrome 7.0.517.44 版浏览器中修复的 12 个安全漏洞包括两个与 SVG(可缩放的矢量图形)有关的安全漏洞、一些解释二维矢量图形的 XML 技术规范中的安全漏洞、一个在 Chrome V8 JavaScript 引擎中的安全漏洞和 3 个与浏览器文本处理有关的安全漏洞。

参考链接: <http://it.people.com.cn/GB/42894/196086/13156111.html>

3、微软公布安全公告 用户应关注未修补漏洞

微软本周发布了 3 项安全公告,涉及 Microsoft Office 和 Forefront Unified Access Gateway 中的 11 个漏洞。其中一个公告被列为微软最高威胁等级“严重”,“严重”等级公告涉及针对 Office 的安全漏洞,在等级为“重要”的第二项安全公告中包含针对 Microsoft Office PowerPoint 2002、PowerPoint 2003 以及 Microsoft PowerPoint Viewer 的漏洞补丁程序。第三项安全公告的威胁等级也为“重要”,该公告涉及 Forefront Unified Access Gateway 2010 中的漏洞,Forefront Unified Access Gateway 是一款适用于企业网络的 VPN 和远程解决方案。

参考链接: <http://it.sohu.com/20101112/n277567459.shtml>

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