

信息安全漏洞周报

2011 年 2 月 7 日-2011 年 2 月 13 日

会 员 版

2011年第6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 113 个，其中高危漏洞 44 个、中危漏洞 24 个、低危漏洞 45 个。上述漏洞中，可被利用于实施远程攻击的漏洞有 98 个；网上已经出现的重要零日攻击代码有 2 个，分别是“Kolibri WebServer HTTP 请求处理缓冲区溢出漏洞”和“ProFTPD 'mod_sftp'模块整数溢出漏洞”。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 81 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 产品漏洞

本周，Microsoft 发布了 2011 年 2 月份的月度例行安全公告，共包含 12 个累积安全更新。其中 3 个更新的综合评级为“严重”，其它均为“重要”。本次发布的安全更新修复了 Microsoft Windows, Office, Internet Explorer 和 IIS 中存在的 22 个漏洞，攻击者可以利用这些漏洞远程执行代码，窃取敏感信息或提升权限。CNVD 收录的具体漏洞包括：Microsoft Excel Axis 属性远程代码执行漏洞、Microsoft Excel 非法对象类型远程代码执行漏洞、Microsoft PowerPoint OfficeArt 远程代码执行漏洞、Microsoft Internet Explorer DLL 装载任意代码执行漏洞、Microsoft Visio 对象内存破坏(CVE-2011-0092)远程代码执行漏洞、Microsoft VBScript 和 JScript 脚本引擎信息泄漏漏洞、Microsoft Windows OpenType 压缩字体格式远程代码执行漏洞、Microsoft Windows 内核整数截断本地特权提升漏洞、Microsoft Windows Kerberos unkeyed 校验本地特权提升漏洞等。CNVD 提醒广大微软用户尽快下载安装补丁程序，避免引发漏洞相关的网络安全事件。

参考链接：
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04014>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04060>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04061>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04062>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04128>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04140>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04138>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04136>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04134>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04129>

2、Adobe 产品安全漏洞

Flash Player 是一款 Flash 文件处理程序；ColdFusion 是一款网络应用服务器开发环境；Shockwave Player 是一款用于播放使用 Director Shockwave Studio 制作的网页外挂软件。本周，Adobe 的产品 Flash Player、Shockwave Player 和 ColdFusion 均出现了多个安全漏洞。CNVD 收录的 Adobe 漏洞包括：Adobe Flash Player 内存破坏漏洞（CVE-2011-0574、CVE-2011-0573、CVE-2011-0572、CVE-2011-0561、CVE-2011-0608）、Adobe Shockwave C SWV 块子结构偏移值远程代码执行漏洞、Adobe ShockwaveFFFFFF88 记录计数元素远程代码执行漏洞、Adobe ColdFusion 存在输入过滤漏洞、Adobe Flash Player 字体解析漏洞、Adobe Flash Player 库装载漏洞等。攻击者可以利用漏洞在受影响的程序中执行任意代码。目前，Adobe 已经发布了这些漏洞的修补程序，CNVD 提醒广大用户尽快下载安装补丁程序，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04147>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04146>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04145>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04144>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04143>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04102>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04101>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04089>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04082>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04081>

3、Kolibri WebServer HTTP 请求处理缓冲区溢出漏洞

Kolibri WebServer 是一款 WEB 服务程序。Kolibri WebServer 在处理包含超长字符串的 GET 或 HEAD 请求可触发基于栈的缓冲区溢出，攻击者可以利用漏洞在受影响的程序中执行任意代码。此漏洞的综合评级为“高危”。目前互联网上已经出现了针对该漏洞的攻击代码，受影响的主要是 Kolibri WebServer 2.x 版本。目前厂商未发布该漏洞的补丁程序，CNVD 建议用户及时关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04049>

4、IBM 产品安全漏洞

IBM Lotus Domino 服务器是一款基于 WEB 合作的应用程序架构，主要用于构建办公自动化系统。IBM Informix Dynamic Server 是一款数据库服务程序。IBM Lotus Connections 是一款基于 J2EE 的社会协作服务软件。本周，IBM 的产品 Lotus Domino、Lotus Notes、Informix IDS、Rational Team Concert 均出现了多个安全漏洞。CNVD 收录的漏洞包括：IBM Lotus Domino 'nLDAP.exe'远程缓冲区溢出漏洞、IBM Lotus Domino iCalendar Meeting 请求解析远程栈缓冲区溢出漏洞、IBM Lotus Domino Server 'diop'远程代码 GIOP getEnvironmentString 处理漏洞、IBM Lotus Connections Wikis 跨站脚本漏洞。攻击者可以利用漏洞窃取敏感信息、劫持目标用户会话或在受影响的程序中执行任意代码。其中，“IBM Lotus Domino 'nLDAP.exe'远程缓冲区溢出漏洞、IBM Lotus Domino iCalendar Meeting 请求解析远程栈缓冲区溢出漏洞、IBM Lotus Domino Server 'diop'远程代码 GIOP getEnvironmentString 处理漏洞”的综合评级为“高危”。目前，除了“IBM Lotus Connections Wikis 跨站脚本漏洞”外，厂商均未发布其它漏洞的补丁信息，CNVD 提醒广大 IBM 用户随时关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04056>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04055>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04054>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04047>

5、HP 产品安全漏洞

HP Power Manager 是惠普公司一套基于 Web 应用，允许管理员通过基于浏览器的控制台管理 HP UPS 的软件解决方案。HP Data Protector 是一款企业级数据保护平台软件。本周，HP Power Manager、Data Protector Manager 和 OpenView Storage Data Protector 产品存在多个综合评级为“高危”的漏洞。攻击者可以利用漏洞在受影响的程序中执行任意代码。CNVD 收录的漏洞包括：HP Power Manager 跨站请求伪造漏洞、HP Data Protector 远程代码默认监听随机 TCP 端口的 Cell manager 服务存在漏洞、HP Data Protector 远程代码 EXEC_CMD 命令实现存在漏洞、HP Data Protector 远程代码 EXEC_CMD 命令过滤器存在漏洞、HP Data Protector 远程代码文件校验漏洞。目前，除了“HP PowerManager 跨站请求伪造漏洞”以外，厂商尚未发布其余漏洞的补丁程序，CNVD 提醒广大用户及时关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04045>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04044>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04043>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04042>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04041>

小结:Microsoft 发布了 2011 年 2 月份的月度例行安全公告,修复了 Microsoft Windows, Office, Internet Explorer 和 IIS 中存在的 22 个漏洞,其中包括危害较大的 IE “圣诞”漏洞, Windows 图形渲染引擎漏洞以及一个存在长达 19 年却未曾披露的 Windows “长老”漏洞。Adobe 发布了多个补丁程序,用于修复 Flash Player、Shockwave Player 和 ColdFusion 多个产品的安全漏洞。另外, Kolibri WebServer 被披露存在一个高危漏洞,互联网上已经出现了针对该漏洞的攻击代码。HP 和 IBM 产品也出现多个安全漏洞,对互联网用户的信息安全和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、Google 发布升级程序,修补了 Google Chrome 的多个安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周, Google 发布多个升级程序用于修补了 Google Chrome 的多个安全漏洞,避免远程攻击者可以利用漏洞使应用程序崩溃或在受影响的程序中执行任意代码。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/2884>

本周要闻速递

1. 微软修复潜伏期长达 19 年的 Windows “长老”漏洞

2 月 9 日,微软 2 月份安全更新发布了 12 个安全补丁,一举修复了 22 处漏洞,其中包括一个潜伏期长达 19 年的 Windows “长老”漏洞(MS11-011),微软为此向全球首先发现该漏洞的国内安全厂商公开致谢。微软 2 月安全公告显示,本月漏洞补丁有 3 个“严重”级别、9 个“重要”级别,危害较大的 IE “圣诞”漏洞、Windows 图形渲染引擎漏洞本次得到了修复。这两个漏洞的信息都已经在网上公开曝光多日,而本次公告中最值得关注的,是一个以潜伏期之长、威胁程度之高而刷新纪录的“长老”漏洞。

参考链接: <http://tech.sina.com.cn/it/2011-02-11/09555166877.shtml>

2. 微软 Windows 高危漏洞威胁隐私,安全专家提醒用户谨慎使用补丁

微软公司已证实 Windows 操作系统 MHTML 协议中存在一个高危 0day 漏洞,可能导致用户电脑中的常用密码、电子邮件等重要信息泄露,此问题将影响全球 9 亿 IE 浏览器用户。最常见的攻击方式是:黑客通过聊天工具、论坛等形式发布一个恶意的网址链接,诱惑网民点击登陆。这个链接看起来是一家知名网站的页面,实际上一点开就会运行恶意脚本,从而窃取网民电脑中的 Cookie 文件等重要信息,对受害者的个人隐私、帐号等造成严重

重威胁。针对微软官方提供的临时补丁，安全专家表示，该补丁是通过“锁定 MHTML 协议”的方式防范漏洞攻击，但同时也可能会导致部分知名网站的正常功能出现兼容性问题。为此，安全专家提醒网民，一旦安装微软临时补丁后遇到某些网站功能失效时，可随时下载微软官方提供的“撤销锁定 MHTML”的恢复工具，就能轻而易举地撤销之前的 MHTML 漏洞临时补丁。根据微软刚发布的 2 月补丁信息推测，微软方面最快要到 3 月份才可能推出 MHTML 漏洞的正式补丁。

参考链接：http://tech.ccidnet.com/art/1099/20110211/2308853_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