

信息安全漏洞周报

2011 年 1 月 24 日-2011 年 1 月 30 日

2011 年第 4 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 99 个，其中高危漏洞 30 个、中危漏洞 22 个、低危漏洞 47 个。上述漏洞中，可利用来实施远程攻击的漏洞有 86 个。经跟踪发现，网上已经出现针对“Microsoft Windows MHTML 脚本代码注入漏洞”和“WordPress Recip.ly "uploadImage.php"任意文件上传漏洞”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。本周收录的漏洞中，已有 63 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 Windows 存在 MHTML 脚本代码注入漏洞

本周，Microsoft 发布安全公告，称在 Windows 平台下 MHTML 存在一个高危 0day 漏洞。该漏洞影响产品包括 Windows XP、Windows Vista、Windows 7 和 Windows Server 2003、Windows 2008 在内的所有 Windows 版本。漏洞存在于 Windows 的 MHTML 协议处理器中，攻击者可利用漏洞在 IE 中运行恶意代码，导致用户信息泄露甚至主机权限被控制。目前，互联网上已经出现针对该漏洞的攻击代码，微软表示正在对漏洞进行研究。在官方正式补丁未发布之前，建议用户通过运行微软操作系统 Fixit 工具来关闭 MHTML 协议处理器。CNVD 提醒广大用户随时关注厂商主页，以获取最新解决方案，避免漏洞引发安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03961>

2、OpenOffice 存在多个远程代码执行漏洞

OpenOffice 是一款开源的文字处理软件。本周，OpenOffice 被披露存在多个“高危”远程代码执行漏洞。漏洞影响 OpenOffice 3.1、3.2、3.2.1、3.2.2 多个版本。远程攻击者可以利用漏洞以应用程序权限执行任意代码或覆盖系统文件。CNVD 收录的漏洞包括：Open Office 任意代码执行漏洞、OpenOffice 处理 TGA 图像存在漏洞、OpenOffice 堆缓冲区溢出

漏洞、OpenOffice 远程代码执行漏洞、OpenOffice 处理 word 文档列表数据存在漏洞、OpenOffice 处理 word 文档列表数据存在漏洞、OpenOffice 释放后使用漏洞（CVE-2010-3452、CVE-2010-3451）、OpenOffice 目录遍历漏洞。目前，厂商已经提供了 OpenOffice 软件升级包用于修复上述漏洞，CNVD 提醒广大用户及时下载更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03939>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03938>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03937>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03936>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03935>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03934>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03933>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03932>

3、Mozilla Bugzilla 发布公告修复多个安全漏洞

Mozilla Bugzilla 是一款基于 Web 的程序 BUG 跟踪系统。本周，Mozilla Bugzilla 发布安全公告，修复了 Mozilla Bugzilla 多个版本中存在的多个安全漏洞。利用这些漏洞，远程攻击者可以进行脚本注入、HTTP 应答分片、跨站请求伪造等攻击，导致用户敏感信息泄漏或权限被窃取。CNVD 收录的漏洞包括：Bugzilla 跨站请求伪造攻击漏洞、Bugzilla 缺少过滤漏洞（CVE-2010-4570、CVE-2011-0048、CVE-2010-4567、CVE-2010-4411、CVE-2010-2761、CVE-2010-4572）、Bugzilla 存在相关不充分随机数未明漏洞。目前，Bugzilla 3.2.10、3.4.10、3.6.4 和 4.0rc2 版本已修复漏洞，CNVD 提醒广大用户及时升级。对于无法升级的用户，可参考厂商主页下载补丁更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03911>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03910>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03909>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03908>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03907>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03906>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03905>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03904>

4、Symantec 多个产品存在安全漏洞

本周，Symantec 多个产品 AntiVirus Corporate Edition、System Center 和 Quarantine Server 出现了多个“高危”安全漏洞。攻击者可以利用漏洞实施执行任意代码攻击。CNVD 收录的漏洞包括：Symantec 多个产品 HDNLR SVC.EXE 服务存在漏洞、Symantec 多个产品'pagehndl.dll'模块执行任意指令漏洞、Symantec 多个产品'pagehndl.dll'模块缓冲区溢出漏洞、Symantec Intel Alert Originator 服务 iao.exe 远程代码执行漏洞、Symantec Intel Alert Man

agement System(CVE-2010-0110)缓冲区溢出漏洞。目前，厂商已经发布了补丁程序修复这些漏洞，CNVD 提醒广大用户及时下载更新，避免引发漏洞相关的安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-03958>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03957>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03956>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03955>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03941>

5、Novell 多款产品出现安全漏洞

本周，Novell 的产品 ZENworks Handheld Management、Groupwise、Groupwise Internet Agent 均出现了安全漏洞。攻击者可以利用漏洞在受影响的应用程序中运行任意代码或窃取系统权限。CNVD 收录的 Novell 漏洞包括：Novell ZENworks Handheld Management 访问点'ZfHPCND.exe'缓冲区溢出漏洞、Novell GroupWise Internet Agent TZID 变量解析漏洞、Novell GroupWise Internet Agent REQUEST-STATUS 缓冲区溢出漏洞。这些漏洞的安全等级均为“高危”。目前，Novell 已经发布了补丁修复了这些漏洞，CNVD 提醒广大用户及时下载更新，避免引发漏洞相关的安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-03931>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03930>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03916>

小结：本周，微软 MHTML 协议漏洞是最为严重的一个漏洞，影响到 IE 浏览器的 6.0、7.0、8.0 等版本，由于攻击代码的出现，极有可能在短时间内被黑色地下产业利用发起大规模网络攻击。OpenOffice 出现了多个“高危”远程代码执行漏洞，远程攻击者可以利用漏洞以应用程序权限执行任意代码或覆盖系统文件。Mozilla Bugzilla 发布安全公告，修复了 Mozilla Bugzilla 多个版本中存在的安全漏洞。另外，Symantec 和 Novell 的多个产品均出现了安全漏洞，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、Opera Web Browser 发布升级程序修补了多个安全漏洞

Opera 是一款开放源代码的 WEB 浏览器。本周，Opera Web Browser 发布了升级程序用于修复多个安全漏洞，以避免攻击者利用漏洞破坏内存、执行任意代码，或窃取用户敏感信息。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/2767>

<http://www.cnvd.org.cn/patch/2768>

<http://www.cnvd.org.cn/patch/2769>

<http://www.cnvd.org.cn/patch/2770>

<http://www.cnvd.org.cn/patch/2771>



本周要闻速递

1. 微软警告用户 Windows 中存在高危 0day 漏洞

1月30日消息，据国外媒体报道，微软当地时间周五警告用户称，Windows 的 MHTML 协议处理器中的一处尚未修正的缺陷，黑客可以利用该缺陷窃取用户信息，诱骗用户安装恶意软件。微软安全团队发言人称，“黑客的脚本代码可以收集用户的信息，例如电子邮件。”安全厂商表示，IE 是唯一受到影响的软件，使用缺省配置的火狐和 Chrome 不会受到影响。该漏洞影响包括 Windows XP、Vista 和 Windows 7 的所有 Windows 版本，因此微软开发补丁软件需要时间。微软建议用户通过运行 Fixit 工具关闭 MHTML 协议处理器。

参考链接：http://news.ccidnet.com/art/1366/20110130/2306551_1.html

2. Facebook 存在 API 漏洞，导致用户页面被乱贴

1月28日消息，据国外媒体报道，社交网站 Facebook 表示，该网站的一个 API 漏洞导致 CEO 扎克伯格的粉丝页面遭未经授权的乱贴。据悉此漏洞还导致数量不详的其他用户页面被乱贴，Facebook 对此表示谴责。很巧合的是，周三 Facebook 刚宣布了两个安全强化措施：扩大使用超文本传输协议安全（HTTPS）以及引入社交认证（social authentication）制度，该制度类似于一个验证系统，并以此代替以往仅依赖 Facebook 用户好友照片的方法。Facebook 的一位发言人在电子邮件声明中表示，“一个漏洞导致未经授权的人在很多公共页面上发帖，该漏洞已经得到修复。”

参考链接：<http://tech.qq.com/a/20110129/000062.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