

信息安全漏洞周报

2011 年 1 月 31 日-2011 年 2 月 6 日

2011年第5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 67 个，其中高危漏洞 24 个、中危漏洞 9 个、低危漏洞 34 个。上述漏洞中，可被利用于实施远程攻击的漏洞有 64 个；网上已经出现零日攻击代码的有 2 个，分别是“Network-13 News 跨站请求伪造漏洞”和“Sun Java 浮点值拒绝服务漏洞”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 49 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 的 Windows 操作系统和 Windows Azure 云计算平台出现两个安全漏洞。攻击者可以利用漏洞窃取敏感信息或执行任意程序。CNVD 收录的具体漏洞包括：Microsoft Windows 执行任意程序漏洞、Microsoft Windows Azure Web Role 信息泄漏漏洞。其中，“Microsoft Windows 执行任意程序漏洞”的安全等级为“高危”。目前，这个高危漏洞尚未被修补，微软只发布了“Microsoft Windows Azure Web Role 信息泄漏漏洞”的补丁，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-2011-04014>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03969>

2、Google Chrome 安全漏洞

Google Chrome 是一款由 Google 公司开发的 WEB 浏览器。本周，Google Chrome 出现多个安全等级为“高危”的漏洞，攻击者可以利用漏洞进行拒绝服务或执行任意代码攻击。CNVD 收录的 Google 漏洞为：Google Chrome 音频处理漏洞、Google Chrome 文件数据更改漏洞、Google Chrome 跨源拖放操作漏洞、Google Chrome PDF 事件处理器漏洞、Google Chrome 内存释放后使用漏洞、Google Chrome 信息泄露漏洞。受上述漏洞影响的

产品包括 Google Chrome 9.0.597.84 之前的多个版本。目前，Google 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，以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-2011-04020>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04019>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04018>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04017>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04016>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04015>

3、Cisco 网络会议产品安全漏洞

本周，Cisco 的 Tandberg 视频会议系统和 WebEx 网络会议解决方案出现了多个安全漏洞。CNVD 收录的 Cisco 漏洞包括：Cisco TANDBERG C 系列和 E/EX 系列默认帐户验证绕过漏洞、Cisco WebEx 远程栈缓冲区溢出漏洞、Cisco WebEx ATP 文件远程栈缓冲区溢出漏洞。攻击者可以利用这些漏洞获取 root 权限或在受影响的程序中执行任意代码。其中“Cisco WebEx 远程栈缓冲区溢出漏洞”和“Cisco WebEx ATP 文件远程栈缓冲区溢出漏洞”的风险等级为“高”，目前厂商已发布这些漏洞的补丁程序，CNVD 建议用户及时下载更新，以避免引发漏洞相关的安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-03998>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03978>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03977>

4、IBM 产品漏洞

本周，IBM 的产品 Rational Build Forge 和 DB2 Universal Database Server 出现了多个安全漏洞。DB2 Universal Database Server 是一款大型的商业关系数据库系统，Rational Build Forge 是一款自动化流程执行软件。CNVD 收录的漏洞包括：IBM Rational Build Forge 跨站脚本漏洞、IBM DB2 Administration Server (DAS) 'validateUser()' 栈缓冲区溢出漏洞、IBM DB2 DBADM 特权丢弃安全绕过漏洞、IBM DB2 db2dasrrm receiveDASMessage 远程代码执行漏洞。攻击者可以利用漏洞窃取敏感信息、劫持目标用户会话、绕过安全限制执行特权操作，或在受影响的程序中执行任意代码。其中，“IBM DB2 Administration Server (DAS) 'validateUser()' 栈缓冲区溢出漏洞”和“IBM DB2 db2dasrrm receiveDASMessage 远程代码执行漏洞”的风险等级为“高危”。目前，IBM 已经发布了这些漏洞的补丁程序，CNVD 建议广大用户及时下载更新，以避免引发漏洞相关的安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-04022>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04004>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04001>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03974>

5、SigPlus Pro ActiveX 控件安全漏洞

SigPlus Pro ActiveX 控件是一款用于文档电子签名的应用插件。本周，SigPlus Pro ActiveX 控件出现多个安全等级为“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：SigPlus Pro ActiveX 控件当处理"SetTabletPortPath()"方法时存在漏洞、SigPlus Pro ActiveX 控件的"SetLogFilePath()"存在文件创建漏洞、SigPlus Pro ActiveX 控件处理"SetLocalIniFilePath()"方法存在漏洞、SigPlus Pro ActiveX 控件处理"KeyString"属性存在漏洞。目前，厂商已经发布了这些漏洞的补丁程序，CNVD 提醒广大用户及时下载更新，以避免引发漏洞相关的安全事件。。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04031>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04029>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04027>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04026>

小结：本周，本周，Microsoft 的 Windows 操作系统和 Azure 云计算平台出现两个安全漏洞。攻击者可以利用漏洞窃取敏感信息或执行任意程序。Google Chrome 出现多个“高危”漏洞，攻击者可以利用漏洞进行拒绝服务或任意代码执行攻击。另外，Cisco WebEx、IBM DB2 和 SigPlus Pro ActiveX 等产品也出现了多个“高危”的安全漏洞，对互联网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、Apache 发布升级程序,修补了 CouchDB 和 Tomcat 的多个安全漏洞

Apache Tomcat 是一款开放源码的 JSP 应用服务器程序，Apache Software Foundation CouchDB 是一款面向文档的数据库管理系统。本周，Apache 发布多个升级程序用于修补了 CouchDB 和 Tomcat 的多个安全漏洞，避免攻击者利用此漏洞发起执行任意代码、劫持目标用户会话、窃取敏感信息或拒绝服务攻击。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/2784>
<http://www.cnvd.org.cn/patch/2801>
<http://www.cnvd.org.cn/patch/2802>
<http://www.cnvd.org.cn/patch/2804>
<http://www.cnvd.org.cn/patch/2810>



本周要闻速递

1. 网页版 Android 应用程序商店可能存在安全漏洞

据国外媒体报道，英国安全厂商当地时间 4 日声称新的网页版 Android 应用程序商店可能存在安全漏洞。不过鉴于网页版 Android 应用程序商店的工作模式，业内人士认为事实上上述问题不会对用户产生太大影响。根据资料，正常情况下用户在 Android 应用程序商店选定一款应用程序并同意其安装之后，该程序将会被迅速下载到用户的手机之中；不过，当用户在使用网页版 Android 应用程序商店时，一旦选择通过网页为手机安装应用程序，其将默认用户允许将该程序安装进手机中，而此时用户根本无法选择不安装。安全厂商认为如果用户的谷歌账户密码在丢失之后此项安全漏洞很可能被黑客所利用，其将在用户不知情的情况下为手机安装恶意程序以窃取用户的个人隐私资料。另一方面，业内人士指出网页版 Android 应用程序商店事实上只是一个 Android 应用程序商店的网络入口，这也就意味着除非恶意程序原本就已经存在于 Android 应用程序商店之中，否则任何人也无法将程序下载进 Android 手机中。

参考链接：<http://www.vccn.com.cn/news/166.html>

2. 微软下周将发布 2 月份的安全公告

微软在今年一月份的“Patch Tuesday”（月度例行补丁发布日）仅发布了两款安全漏洞补丁。但在二月份，这一数字将大大增加。日前微软就宣布，将在美国当地时间 2 月 8 日周二，北京时间 2 月 9 日清晨发布二月份的 12 个安全补丁。在这 12 个安全补丁当中，3 个为最高级别严重级，9 个为重要级。这些补丁共修复了 Windows、IE、Office、Visual Studio 和 IIS 中存在的 22 个安全漏洞，其中涉及安全通报 2490606 描述的图像呈现引擎漏洞，安全通报 2488013 描述的 IE 浏览器安全漏洞，以及 IIS 7.0 和 7.5 中的 FTP 服务安全问题等。涉及操作系统方面，12 个补丁中有一个针对各操作系统版本中的 IE 浏览器，一个针对 Office Visio 软件，Windows XP 将收到 8 个补丁，Vista 的补丁数为 6 个，Windows 7 则有 7 个补丁。

参考链接：<http://www.uuzo.cn/News/26773.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