

信息安全漏洞周报

2011 年 5 月 23 日-2011 年 5 月 29 日

2011年第21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 89 个，其中高危漏洞 51 个、中危漏洞 37 个、低危漏洞 1 个。上述漏洞中，可利用来实施远程攻击的漏洞有 85 个。网上已经出现针对“Gadu-Gadu Instant Messenger 文件传输跨站脚本漏洞”、“ClipBucket SQL 注入漏洞”等的零日攻击代码，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 47 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。

成员单位报送漏洞统计

本周，共有 6 家成员单位报送了本周收录的全部 89 个漏洞，各单位报送情况如表 1 所示。其中，启明星辰、恒安嘉新、东软、绿盟科技报送的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	46	0
绿盟科技	3	0
恒安嘉新	41	0
东软	4	0
安氏领信	1	0
安天	1	0
总计	89（去重）	0

表 1 成员单位上报漏洞统计表

本周，CNVD 整理和发布的漏洞涉及 Cisco、Google、Avaya Inc.、HP、IBM 等多家厂商的产品，漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Cisco	7	7.9%
2	Google	5	5.6%
3	Avaya Inc.	4	4.5%
4	HP	3	3.4%
5	IBM	2	2.2%
6	Apache	2	2.2%
7	ISC	1	1.1%
8	Adobe	1	1.1%
9	7-Technologies	1	1.1%
10	其他	63	70.9%

表 2 漏洞产品涉及厂商分类统计

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、Cisco 产品安全漏洞

Cisco Content Delivery System 是一款思科公司开发的内容分发系统解决方案；Cisco IOS XR 是 Cisco IOS 软件家族的一员，使用基于微内核的操作系统架构；Cisco RVS4000 /WRVS4400N 是千兆级路由器。本周，上述 Cisco 产品存在多个安全漏洞。攻击者可以利用漏洞发起拒绝服务攻击，使服务器停止响应或注入任意命令，获取敏感信息。CNVD 收录的相关漏洞包括：Cisco CDS Internet Streamer Web 服务器远程拒绝服务漏洞、Cisco IOS XR NetIO 进程远程拒绝服务漏洞、Cisco IOS XR SSHv1 '/tmp/ssh_lock'远程拒绝服务漏洞、Cisco IOS XR SPA 接口处理器远程拒绝服务漏洞、Cisco RVS4000/WRVS4400N Web 管理接口私/共钥信息泄露漏洞、Cisco RVS4000/WRVS4400N Web 管理接口命令注入漏洞、Cisco RVS4000/WRVS4400N Web 管理接口信息泄露漏洞。上述漏洞的综合评级均为“高危”。厂商已经发布了这些漏洞的补丁程序，CNVD 提醒相关用户请及时获取补丁程序进行修补。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05593>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05592>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05591>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05590>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05589>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05588>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05587>

2、Google Chrome 安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，Google Chrome 被披露存在多个安全漏洞，攻击者可以利用漏洞绕过安全限制，破坏内存或在受影响的程序中执行任意代码。CNVD 收录的漏洞包括：Google Chrome 跨站脚本过滤器安全绕过漏洞、Google Chrome Blob 处理越界远程代码执行漏洞、Google Chrome GPU 命令缓冲区内内存破坏漏洞、Google Chrome 浮点渲染内存破坏漏洞、Google Chrome 弹出窗口拦截器安全绕过漏洞。其中“Google Chrome Blob 处理越界远程代码执行漏洞、Google Chrome GPU 命令缓冲区内内存破坏漏洞、Google Chrome 浮点渲染内存破坏漏洞”的综合评级为“高危”。除“Google Chrome 跨站脚本过滤器安全绕过漏洞”外，厂商已经发布其余漏洞的补丁程序，CNVD 提醒相关用户及时获取补丁程序进行修补。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05603>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05577>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05576>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05575>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05574>

3、Joomla 组件安全漏洞

Joomla 是一套开源的内容管理系统。本周，Joomla 的多款组件 Map Locator、Comp Restaurante、com_joomnik、com_jmsfileseller 存在多个 SQL 注入漏洞。攻击者可以利用漏洞注入任意 SQL 命令，执行 SQL 查询，获得网站系统管理权限。CNVD 收录的相关漏洞包括：Joomla 组件 com_jmsfileseller SQL 注入漏洞、Joomla 组件 com_joomnik SQL 注入漏洞、Joomla 和 Mambo Comp Restaurante 组件'id'参数 SQL 注入漏洞、Joomla 组件 Map Locator "cid" SQL 注入漏洞。上述漏洞的综合评级均为“高危”，且部分漏洞的攻击代码已在互联网出现。厂商尚未发布这些漏洞的补丁程序，CNVD 提醒广大用户随时关注厂商主页获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05633>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05632>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05628>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05626>

4、ISC BIND 9 RRSIG 查询类型远程拒绝服务漏洞

ISC BIND 是应用广泛的域名服务系统软件。ISC BIND 由于未能正确处理某些资源记录，存在一个远程拒绝服务漏洞。攻击者可利用此漏洞发起拒绝服务攻击，使其无法对合法用户提供服务。此漏洞的综合评级为“高危”。目前，厂商已经发布漏洞的补丁程序，CNVD 提醒相关用户及时获取补丁程序进行修补。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-05615>

5、Gadu-Gadu Instant Messenger 文件传输跨站脚本漏洞

Gadu-Gadu 是一款在线即时聊天程序。Gadu-Gadu 由于未能正确处理文件传送请求,可在文件名中构造 255HTML 代码字符(无斜杠),通过特制的文件发送请求报文将 JavaScript 注入到用户应用软件 UI。其中的 Javascript 代码可用于触发多种恶意行为,如保存和运行目标主机上的任意文件。由于攻击时使用了 Javascript 代码, ASLR 或 DEP 等操作系统安全机制不能完全防范此类攻击。目前,互联网上已经出现针对该漏洞的攻击代码,主要影响 Gadu-Gadu 7.7 版本和 Instant Messenger 多个版本。厂商尚未发布该漏洞的补丁程序,CNVD 提醒广大用户随时关注厂商主页获取最新版本。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-05573>

小结: 本周, CNVD 收录了 Cisco 产品 Content Delivery System、IOS XR 和 RVS400 0/WRVS4400N 的多个综合评级为“高危”的漏洞,攻击者可以利用漏洞发起拒绝服务攻击,使服务器停止响应或注入任意命令,获取敏感信息。Google 修复了 Chrome 存在的多个安全漏洞。同时, CNVD 还收录了 Joomla 多个组件存在的漏洞、ISC BIND 拒绝服务漏洞以及 Gadu-Gadu 即时聊天程序零日漏洞,这些对使用这些产品的用户构成较大威胁。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、IBM 发布升级程序, 修补多个产品安全漏洞

本周, IBM 发布升级程序, 修补了 Lotus Notes、Websphere Portal、Web Content Management 多个产品存在的安全漏洞。远程攻击者可以利用漏洞发起跨站脚本攻击, 获取敏感信息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/3946>

<http://www.cnvd.org.cn/patch/3947>

本周要闻速递

1. IE 浏览器曝出漏洞 易导致账号和密码泄露

据报道, 国外研究人员近日发现 IE 浏览器存在名为 cookiejacking 的安全漏洞, 容易导致用户帐号信息泄露。经过验证, 该漏洞可能被黑客用来针对特定目标实施盗号, 微博名人尤其要注意保护帐号安全, 不可轻易点击陌生人发布的可疑网址。安全专家介绍说,

cookiejacking 漏洞被攻击有两个前提条件：第一，使用 IE 系列浏览器打开恶意网页；第二，在网页中进行鼠标拖拽操作，黑客可能会设计一个网页游戏，比如把一个篮球移动到篮筐里，诱骗受害者进行相应的操作。一旦漏洞攻击成功，黑客可以得到存储在浏览器文件中的 cookie。由于很多人在登录微博、Gmail 邮箱等帐号时会选择“记住密码”，cookie 失窃就意味着这些帐号很可能会遭黑客窃取。根据国外的漏洞发现者测试，他在 Facebook 上公布了一个“拖拽美女衣服”的游戏，150 名好友中有 80 多人上钩，使其收集到了这些好友的 IE 浏览器 cookie 文件。安全建议指出，在该漏洞得到修复前，IE 用户应避免在陌生网站上进行网页游戏，以免落入黑客陷阱。。

参考链接：<http://www.7747.net/News/201105/91974.html>

2. Chrome 网店系统存在安全漏洞

日前，安全专家大卫·罗杰斯批评谷歌 Chrome 浏览器额外添加的网店系统。他表示，该系统存在与 Android 手机操作系统相同的安全隐患。据悉，凡是从 Chrome 网店上下载安装的应用程序都要求成套的用户系统权限，例如游戏“超级玛丽”1 代和 2 代的非官方控制台端口要求掌握用户浏览器的历史、书签和“用户浏览过的所有网站的数据”的权限而控制台对“用户浏览过的所有网站的数据”的要求当中就含有大量不安定因素。而谷歌发表的权限声明，控制台通过这些 Flash 游戏端口，可以了解到用户在任何时间任何地点访问的任何网站，其中甚至包括用户的网银信息、个人网页邮箱以及个人 Facebook 主页等。除此之外，这些应用程序还可以通过在其他网站保存的 Cookies 从而探测到该类网站所属性质。虽然目前 Chrome 网店已撤销了超级玛丽两款游戏的下载，不过该游戏是否真正侵犯了用户的安全隐私，目前还无法明确。

参考链接：<http://www.cnbeta.com/articles/144218.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