

信息安全漏洞周报

2012 年 2 月 27 日-2012 年 3 月 4 日

2012 年 第9 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 127 个，其中高危漏洞 43 个、中危漏洞 80 个、低危漏洞 4 个。上述漏洞中，可利用来实施远程攻击的漏洞有 108 个。本周收录的漏洞中，已有 62 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。本周互联网上出现“Google V8 服务端 JavaScript 注入漏洞”、“BrewBlogger 存在多个文件上传漏洞”等的零日攻击代码，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 6 家成员单位和 2 家合作伙伴单位报送了本周收录的全部 127 个漏洞。各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰、安天实验室报送数量较多。此外，本周 CNVD 接收到 JPCERT/CC、绿盟科技广西分公司漏洞研究者报送的两个国产应用软件系统漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	91	0
绿盟科技	84	1
恒安嘉新	35	0
安天实验室	28	0
天融信	7	0
安氏领信	4	0
JPCERT/CC	1	1
总计	127（去重）	2

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cisco、IBM、NetEase 等多家厂商的产品，部分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	11	8.7%
2	IBM	9	7.1%
3	NetEase	5	3.9%
4	Dotclear	5	3.9%
5	Linux	4	3.1%
6	PostgreSQL	3	2.4%
7	phpDenora	3	2.4%
8	LimeSurvey	3	2.4%
9	Codeorigin	2	1.6%
10	freelancerKit	2	1.6%
11	其它	80	62.9%

表 2 漏洞产品涉及厂商分布统计表

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. IBM 安全漏洞

本周，IBM 的多款产品 Tivoli Provisioning Manager Express、WebSphere Application Server、Personal Communications 等被披露存在多个安全漏洞。远程攻击者可以利用漏洞管理数据和管理员密码、上传文件、以系统权限执行任意代码或使应用程序崩溃。CNVD 收录的相关漏洞包括：IBM Tivoli Provisioning Manager Express ActiveX 控件远程代码执行漏洞、IBM Tivoli Provisioning Manager Express SQL 注入漏洞（CNVD-2012-10291、CNVD-2012-10290、CNVD-2012-10292、CNVD-2012-10293）、IBM WebSphere Application Server for z/OS JAX-RPC 存在未明漏洞、IBM Personal Communications '.ws'文件'pcspref.dll'远程栈缓冲区溢出漏洞、IBM AIX ICMP 报文处理拒绝服务漏洞。其中，除“IBM WebSphere Application Server for z/OS JAX-RPC 存在未明漏洞”、“IBM AIX ICMP 报文处理拒绝服务漏洞”外，其余漏洞的综合评级均为“高危”。目前，IBM 已经发布这些漏洞的修补程序，CNVD 提醒相关用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42115
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42276

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42277
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42275
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42278
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=42280
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41575
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41335

2. 网易产品安全漏洞

本周，用于 Android 系统上的网易微博、网易阅读应用、网易手机邮、网易云相册、网易微博 HD 被披露存在安全漏洞，目前没有详细漏洞细节提供。CNVD 收录的相关漏洞包括：网易微博存在漏洞、网易阅读存在漏洞、网易手机邮存在漏洞、网易云相册存在漏洞、网易微博 HD 存在漏洞。目前，厂商还未发布上述漏洞的修补程序，CNVD 提醒相关用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41835
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41819
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41817
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41816
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41820

3. Cisco 产品安全漏洞

本周，Cisco 多款产品 Wireless LAN Controller、Unified Communications Manager、Unity Connection、Cius 被披露存在多个安全漏洞。攻击者可以利用漏洞使设备重载并提升权限控制系统。CNVD 收录的相关漏洞包括：Cisco Wireless LAN Controller IPv6 报文处理拒绝服务漏洞（CNVD-2012-10245）、Cisco Unified Communications Manager SCCP 拒绝服务漏洞（CNVD-2012-10232）、Cisco Unity Connection TCP 段拒绝服务漏洞、Cisco Wireless LAN Controller HTTP 请求拒绝服务漏洞（CNVD-2012-10243）、Cisco Cius 远程拒绝服务漏洞、Cisco TelePresence Video Communication Server 会话拒绝服务漏洞（CNVD-2012-10229、CNVD-2012-10230）、Cisco Unity Connection 远程特权提升漏洞（CNVD-2012-10239）。上述漏洞的综合评级为“高危”。目前，Cisco 已经发布上述漏洞的修补程序，CNVD 提醒相关用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41858
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41815
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41838
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41856
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41775
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41795

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41796

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41836

4. Linux Kernel 安全漏洞

Linux 是一款开源的操作系统。本周，Linux 内核被披露存在多个安全漏洞，本地攻击者可以利用漏洞使系统崩溃或通过符号链接破坏系统文件。CNVD 收录的相关漏洞包括：Linux Kernel TOMOYO LSM 本地拒绝服务漏洞、Linux Kernel 本地拒绝服务漏洞（CNVD-2012-10210）、Linux Kernel CIFS 'umount'本地拒绝服务漏洞（CNVD-2012-10211）、Linux 内核'iproute'包不安全临时文件创建漏洞。目前，厂商已经发布上述漏洞的修补程序，CNVD 提醒相关用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41797

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41576

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41577

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=41375

5. Google V8 服务端 JavaScript 注入漏洞

V8 是 Google 的开源 JavaScript 引擎。本周，Google 的 V8 服务器端引擎在实现上存在 SSJS 注入漏洞，攻击者通过 PHP 中的服务器端 JavaScript 注入漏洞可导致注入任意代码。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 V8 JavaScript Engine。厂商尚未发布上述漏洞的修补程序，CNVD 提醒广大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/sites/main/preview/ldgg_preview.htm?tid=41755

更多高危漏洞如表 3 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。

参考链接：<http://www.cnvd.org.cn/publish/main/52/index.html>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2012-10299	Tiny HTTP Server 远程利用漏洞	高	暂无
CNVD-2012-10274	Novell Groupwise Client 地址簿解析远程代码执行漏洞 (CNVD-2012-10274)	高	Novell GroupWise 8.0 Support Pack 2 和 Novell Groupwise 2012 已经修复此漏洞，建议用户下载使用： http://www.novell.com/products/groupwise/
CNVD-2012-10228	Hitachi JP1/Cm2/Network Node Manager i 存在未明远程代码执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.hitachi.co.jp/Prod/comp/soft1/security/info/.vuls/HS12-009/index.ht

			ml http://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/./vuls/HS12-009/index.html
CNVD-2012-10246	用友软件 ICC 客服系统文件上传漏洞	高	暂无
CNVD-2012-10217	CJWSOFT ASPGuest GuestBook 'edit.asp' SQL 注入漏洞	高	暂无
CNVD-2012-10213	NetDecision Traffic Grapher Server 源代码泄露漏洞	高	NetMechanica NetDecision 4.6.1 已经修复此漏洞，建议用户下载使用： http://www.netmechanica.com/products/?cat_id=2
CNVD-2012-10216	Joomla! Dregister 组件'list1'SQL 注入漏洞	高	暂无
CNVD-2012-10193	MyJobList 'eid' SQL 注入漏洞	高	暂无
CNVD-2012-10194	Open Handset Alliance Android 浏览器远程代码执行漏洞	高	暂无
CNVD-2012-10203	Sysax Multi Server 'username'缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，IBM 的多款产品被披露存在多个安全漏洞。远程攻击者可以利用漏洞操作数据，获得管理员密码，上传文件，以系统权限执行任意代码或使应用程序崩溃。网易、Cisco 产品和 Linux 操作系统被披露存在多个安全漏洞，影响涉及广大终端用户以及工业行业用户。而 Google V8 开源 JavaScript 引擎零日漏洞、Web 应用的高危漏洞也需引起相关用户注意，加强防范。此外，本周 CNVD 收录的用友软件 ICC 漏洞影响涉及多个中央企业以及上市公司，目前，暂未发布漏洞补丁，后续情况 CNVD 将继续跟踪。

CNVD 提醒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

CNVD 整理和发布以下重要安全修补信息。

1、Novell 发布升级程序，修补 Groupwise Client 安全漏洞

本周，Novell 发布升级程序，修补了 Groupwise Client 存在的安全漏洞。利用披露的漏洞攻击者可以通过构建恶意 URL，诱使用户打开，以登录用户权限执行任意代码。

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/sites/main/preview/bdgg_preview.htm?tid=11851

本周要闻速递

1.谷歌悬赏奖金查浏览器安全漏洞

美国谷歌公司 28 日宣布，已设立 100 万美元作为奖金，奖励任何能够发现并攻破谷歌 Chrome 浏览器安全漏洞的黑客。据谷歌 Chrome 浏览器安全团队通过博客发布的公告，如果哪个黑客能够找出 Chrome 浏览器的任何全面破解方案，即利用浏览器自身漏洞控制他人用户的电脑，那么他将获得 6 万美元奖金。不过，这一奖金的前提是这名黑客必须提供破解方案的所有细节，同时向谷歌公司以外的第三方保密。除此以外，黑客如能够结合 Chrome 浏览器 Windows 7 系统的漏洞找出破解方案，将获得 4 万美元奖励。根据规则，黑客每找出一个漏洞并提供破解方案，谷歌将按级别支付奖金，但总奖金限额为 100 万美元。谷歌 Chrome 浏览器安全团队称这个项目的目的是能够借此发现全面的破解方案，不仅可以修复漏洞，还能通过了解系统的弱点和破解技巧，更好地为用户提供保护。

参考链接：http://tech.gmw.cn/2012-02/29/content_3677213.htm

2.iOS 存在安全漏洞 应用可无预警获取照片库

最近苹果 iOS 移动操作系统暴安全漏洞，应用开发者可以通过要求获取用户当前位置的对话框来读取用户设备的照片库信息。也就是说，用户简单的一次点击就会让照片库里头的信息赤裸裸的展现给开发者，而开发者无需通知用户便可以轻而易举的将这些信息发送到自己的服务器上。该问题在于 iOS 应用不仅仅有访问用户联系人数据库（包括地址和备注）的权限，还可以对 iOS 应用沙箱中一切信息有着绝对的支配权，包括图片、音乐、视频、日历以及其他数据。所有的这些信息对于开发者来说都是透明的，当他们的应用打开运行的时候，他们完全可以自由地将信息传送到自己的服务器上。事实证明，地址簿并不是唯一容易被获取的东西，照片数据也非常的脆弱。据应用开发者透露，当用户在 iPhone、iPad 或 iPod Touch 上允许某应用访问地理位置信息之后，他们便可以在毫无通知或警告的前提下复制用户整个照片库。目前尚不清楚苹果 App Store 中是否存在有类似小动作的应用。苹果公司表示说，他们会审核并屏蔽那些在没有适当理由的前提下，试图拷贝用户照片库但不获取用户授权的应用。不过值得指出的是，复制地址簿的数据也是苹果规则中禁止的，但是他们还是让不少知名应用这么做了。

参考链接：http://news.xinhuanet.com/tech/2012-03/01/c_122772124.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