

信息安全漏洞周报

2012 年 2 月 13 日-2012 年 2 月 19 日

2012 年 第 7 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 123 个，其中高危漏洞 66 个、中危漏洞 55 个、低危漏洞 2 个。上述漏洞中，可利用来实施远程攻击的漏洞有 115 个。本周收录的漏洞中，已有 106 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“Skype 聊天日志本地信息泄露漏洞”、“jetVideo '.m3u' 文件缓冲区溢出漏洞”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 1 家合作伙伴单位报送了本周收录的全部 123 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。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	128	0
启明星辰	125	0
安天实验室	30	0
东软	5	0
安氏领信	4	0
天融信	3	0
中国电力科学研究院	4	4
总计	123（去重）	4

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、Advantech、Adobe、Oracle、Google 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	Microsoft	20	16.3%
2	Advantech	18	14.6%
3	Adobe	17	13.8%
4	Oracle	12	9.6%
5	Google	12	9.6%
6	RabidHamster	4	3.3%
7	PHP	3	2.4%
8	LEPTON	3	2.4%
9	Debian	3	2.4%
10	11in1	2	1.6%
11	其它	29	24%

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、Microsoft 产品安全漏洞

2 月 14 日，微软发布了 2011 年 2 月份的月度例行安全公告，共包含 9 项更新，共修复了涉及 Microsoft Windows、Internet Explorer、.NET Framework、Silverlight、Office、SharePoint 等多个产品存在的 21 个安全漏洞。利用上述漏洞，攻击者可以远程执行任意代码或提升特权。CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2012-09892）、Microsoft Internet Explorer VML 处理远程代码执行漏洞（CNVD-2012-09893）、Microsoft Windows Kernel GDI 访问冲突本地特权提升漏洞、Microsoft Internet Explorer 跨域信息泄露漏洞（CNVD-2012-09885）、Microsoft Internet Explorer 空字节泄露漏洞、Microsoft Silverlight 和 .NET Framework 堆破坏远程代码执行漏洞、Microsoft Silverlight 和 .NET Framework 未管理对象远程代码执行漏洞、Microsoft Windows C 运行时库缓冲区溢出漏洞。上述漏洞的综合评级均为“高危”。CNVD 提醒广大 Microsoft 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=39458
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39459
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39488
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39451
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39455

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39568

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39588

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39708

2、Adobe Shockwave Player 产品安全漏洞

Adobe Shockwave Player 是一款用于播放使用 Director Shockwave Studio 制作的网页的插件程序。本周，Adobe Shockwave Player 软件被披露存在多个安全漏洞。远程攻击者可以利用漏洞以应用程序上下文执行任意代码。CNVD 收录的相关漏洞包括：Adobe ShockwavePlayer 远程内存破坏漏洞（CNVD-2012-09890、CNVD-2012-09888、CNVD-2012-09887、CNVD-2012-09879、CNVD-2012-09886、CNVD-2012-09884、CNVD-2012-09882、CNVD-2012-09880）。上述漏洞的综合评级均为“高危”。目前，Adobe 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=39456

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39454

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39453

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39431

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39452

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39450

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39448

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39432

3、Oracle 产品安全漏洞

Oracle Sun Java Runtime Environment 是一款为 JAVA 应用程序提供运行环境的应用程序。本周，上述 Oracle 产品被披露存在多个安全漏洞，攻击者可以利用漏洞以应用程序上下文执行任意代码。CNVD 收录的相关漏洞包括：Oracle Java SE 远程栈溢出漏洞、Oracle Java SE 远程任意代码执行漏洞（CNVD-2012-09927、CNVD-2012-09930、CNVD-2012-09931、CNVD-2012-09933、CNVD-2012-09934、CNVD-2012-09935、CNVD-2012-09936）。其中，除“Oracle Java SE 远程栈溢出漏洞”外，其余漏洞的综合评级均为“高危”。目前，Oracle 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=39797

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39798

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39801

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39802

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39804

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39805

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39806

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39807

4、Advantech 产品安全漏洞

Advantech/BroadWin SCADA WebAccess 是一款完全基于浏览器的人机界面(HMI)和监控及数据采集(SCADA)软件,广泛应用于国内外工业行业企业。本周, Advantech WebAccess 被披露存在多个安全漏洞, 远程攻击者可以利用漏洞访问修改数据、执行任意代码或进行拒绝服务攻击。CNVD 收录的相关漏洞包括: Advantech WebAccess SQL 注入漏洞 (CNVD-2012-09951、CNVD-2012-09944、CNVD-2012-09958)、Advantech WebAccess 缓冲区溢出漏洞 (CNVD-2012-09947、CNVD-2012-09949、CNVD-2012-09955)、Advantech WebAccess 文件操作漏洞 (CNVD-2012-09948)、Advantech WebAccess 格式字符串漏洞 (CNVD-2012-09960)。上述漏洞的综合评级均为 “高危”。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=39873

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39889

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39851

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39869

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39877

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39871

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39870

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=39891

5、Skype 聊天日志本地信息泄露漏洞

Skype 是一款流行的 P2P VoIP 软件, 用于即时语音通讯服务。本周, Skype 被披露存在一个信息泄露漏洞。由于 VoIP 对所有聊天消息记录以明文方式存到本地 sqlite3 DB(文件 main.db, 表 Messages)中, 攻击者可以利用漏洞获得敏感信息。目前, 互联网上已经出现针对该漏洞的攻击代码, 主要影响 Skype 5.x 版本。但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=39368

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-2012-09917	Cisco Nexus 设备 IP 栈远程拒绝服务漏洞	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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-2

			0120215-nxos
CNVD-2012-09963	libpng 'png_decompress_chunk()' 远程整数溢出漏洞	高	暂无
CNVD-2012-09919	Debian devscripts 'debdiff' 远程代码执行漏洞 (CNVD-2012-09919)	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.debian.org/security/2012/dsa-2409
CNVD-2012-09875	GNU 的 glibc 时区解析远程整数溢出漏洞	高	目前官方已对此漏洞发布相关补丁和处理方案, 请及时更新软件到最新版本或安装相应补丁: http://www.gnu.org/software/libc/
CNVD-2012-09865	ALFTP 不安全可执行文件装载任意代码执行漏洞	高	ALTools ALFTP 5.31 已经修复此漏洞, 建议用户下载使用: http://www.altools.jp/ETC/NEWS.aspx?mid=231
CNVD-2012-09860	RabidHamster R4 缓冲区溢出漏洞 (CNVD-2012-09860)	高	暂无
CNVD-2012-09854	ImageMagick 缓冲区溢出漏洞	高	ImageMagick 6.7.5-1 已经修复此漏洞, 建议用户下载使用: http://www.imagemagick.org/
CNVD-2012-09856	jetVideo 'm3u' 文件缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

小结: 本周, 微软发布了 2011 年 2 月份的月度例行安全公告, 共包含 9 项更新, 共修复了涉及 Microsoft Windows、Internet Explorer、.NET Framework、Silverlight、Office、SharePoint 等多个产品存在的 21 个安全漏洞。利用上述漏洞, 攻击者可以远程执行任意代码或提升特权。Adobe, Oracle 和 Advantech 的应用产品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。此外, Skype 聊天软件零日漏洞、Cisco 网络设备的高危漏洞需引起相关用户注意, 加强防范。

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、Cisco 发布升级程序, 修补多款产品安全漏洞

本周, Cisco 发布升级程序, 修补了 IronPort Encryption Appliance 和 Nexus 存在的安全漏洞, 避免远程攻击者可以利用漏洞进行跨站脚本和拒绝服务攻击。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/sites/main/preview/bdgg_preview.htm?tid=10078
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=10079

本周要闻速递

1. 公钥加密算法 RSA 存在安全漏洞

据《纽约时报》报道, 欧美数学家和密码学家偶然发现, 目前被全世界广泛应用的公钥加密算法 RSA 存在漏洞。他们发现, 在 700 万个实验样本中有 2.7 万个公钥并不是按理论随机产生的。也就是说, 或许有人可以找出产生公钥的秘密质数。该研究项目的报告称, 绝大多数公钥都是按理论产生的, 但是每一千个公钥中会有两个存在安全隐患。报告称, 为防止有人利用该漏洞, 有问题的公钥已从公众访问的数据库中移除。为确保系统的安全性, 网站需要在终端做出改变。

参考链接: <http://www.kejixun.com/a/2012-02-15/16935.html>

2. 谷歌已修复谷歌钱包漏洞

近日, 谷歌发布一款补丁, 修复了谷歌钱包(Google Wallet)服务中的一处安全漏洞。信息安全公司上周发现了谷歌钱包的一处漏洞, 可导致攻击者获得用户手机控制权, 并窃取用户帐户中的资金。谷歌在一份声明中称, 已经发布一款补丁程序, 可防止入侵者访问谷歌钱包预付费卡。在发现该漏洞后, 谷歌已经停售这种预付费卡, 但从今日开始, 谷歌已重新销售预付费卡。

参考链接: <http://www.techweb.com.cn/news/2012-02-16/1153572.shtml>

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