

信息安全漏洞周报

2012 年 1 月 30 日-2012 年 2 月 5 日

2012 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**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 167 个，其中高危漏洞 46 个、中危漏洞 109 个、低危漏洞 12 个。上述漏洞中，可利用来实施远程攻击的漏洞有 146 个。本周收录的漏洞中，已有 134 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“ComponentOne FlexGrid ActiveX 控件缓冲区溢出漏洞”、“PDF-XChange pdfSaver ActiveX 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 5 家成员单位报送了本周收录的全部 167 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技、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
启明星辰	92	0
绿盟科技	79	0
安天实验室	32	0
安氏领信	3	0
东软	2	0
总计	167（去重）	0

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、FFmpeg、Mozilla 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	Oracle	27	16.2%

2	FFmpeg	15	9.0%
3	Mozilla	11	6.6%
4	Hitachi	5	3.0%
5	Google	5	3.0%
6	Tencent	4	2.4%
7	IBM	3	1.8%
8	Apache	3	1.8%
9	Debian	2	1.2%
10	Novell	1	0.6%
11	其它	167	54.4%

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、Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。本周，上述 Mozilla 产品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、绕过安全限制、获得敏感信息或使应用程序崩溃。CNVD 收录的相关漏洞包括：Mozilla Firefox/SeaMonkey/Thunderbird 跨域安全绕过漏洞、Mozilla Firefox/SeaMonkey/Thunderbird 信息泄露漏洞、Mozilla Firefox/Thunderbird/SeaMonkey nsDOMAttribute 内存错误引用漏洞、Mozilla Firefox/SeaMonkey/Thunderbird Ogg Vorbis 文件内存破坏漏洞、Mozilla Firefox/SeaMonkey/Thunderbird XPCo nnect 安全检查跨域脚本漏洞、Mozilla Firefox/SeaMonkey/Thunderbird 内存破坏漏洞（CNVD-2012-09645、CNVD-2012-09644）、Mozilla Firefox/SeaMonkey/Thunderbird XSLT 样式表拒绝服务漏洞。其中，除“Mozilla Firefox/SeaMonkey/Thunderbird 跨域安全绕过漏洞”、“Mozilla Firefox/SeaMonkey/Thunderbird 信息泄露漏洞”外，其余漏洞的综合评级均为“高危”。目前，Mozilla 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=38097
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38098
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38099
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38101
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38102
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38104

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38103

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38100

2、Hitachi 产品安全漏洞

本周，Hitachi JP1 产品、uCosminexus 产品和 COBOL2002 产品被披露存在多个安全漏洞。远程攻击者可以利用漏洞控制目标用户系统、获得敏感信息。CNVD 收录的相关漏洞包括：Hitachi JP1 产品存在未明跨站脚本漏洞、Hitachi JP1/IT Desktop Management Manager 存在未明跨站脚本漏洞、Hitachi uCosminexus 存在未明跨站脚本漏洞、Hitachi uCosminexus EUR Print Manager 存在未明跨站脚本漏洞、Hitachi COBOL2002 产品存在未明漏洞。目前，Hitachi 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=38089

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38090

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38091

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38092

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38071

3、Google 产品安全漏洞

Google Chrome 是一款开源的 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以应用程序上下文执行任意代码。CNVD 收录的相关漏洞包括：Google Chrome Skia 未初始化漏洞、Google Chrome 堆缓冲区溢出漏洞、Google Chrome 内存错误引用漏洞（CNVD-2012-09670、CNVD-2012-09681、CNVD-2012-09673）。上述漏洞的综合评级均为“高危”。目前，Google 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=38197

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38194

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38189

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38200

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38192

4、FFmpeg 产品安全漏洞

FFmpeg 是一款用于录制、转换和流化音频和视频的编解码处理程序。本周，FFmpeg 存在多个安全漏洞，远程攻击者可以利用漏洞执行任意代码。CNVD 收录的相关漏洞包括：FFmpeg 存在漏洞（CNVD-2012-09580、CNVD-2012-09569、CNVD-2012-09570、CNVD-2012-09571、CNVD-2012-09572、CNVD-2012-09575、CNVD-2012-09578、CNVD-2012-09584）。目前，FFmpeg 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=37998

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37976
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37988
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37989
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37990
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37993
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37996
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38002

5、ComponentOne FlexGrid ActiveX 控件缓冲区溢出漏洞

OPC Systems.NET 是基于.NET 架构的应用于工业控制系统 SCADA\HMI 的产品。本周，ComponentOne FlexGrid ActiveX 控件被披露存在一个缓冲区溢出漏洞，攻击者可以利用漏洞构建恶意链接，诱使用户解析，以应用程序上下文执行任意代码。该漏洞的综合评级为“高危”。目前，互联网上已经出现针对该漏洞的攻击代码，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=38069

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-2012-09689	EMC NetWorker 缓冲区溢出漏洞	高	EMC Networker 7.6.3 SP1 Cumulative Relea 已经修复此漏洞，建议用户下载使用： http://www.emc.com/products/detail/software/networker.htm
CNVD-2012-09668	NX Web Companion 升级处理漏洞	高	暂无
CNVD-2012-09661	Dream Report 远程代码执行漏洞	高	Ocean Data Systems Dream Reports 4.0 已经修复此漏洞，建议用户下载使用： http://www.dreamreport.net/php/download/download.php?lang=en
CNVD-2012-09656	SolarWinds Storage Manager Server SQL 注入漏洞	高	暂无
CNVD-2012-09655	Savant Web Server 远程缓冲区溢出漏洞	高	暂无
CNVD-2012-09654	Caminova DjVu 浏览器插件'Sjbz'块解析缓冲区溢出漏洞	高	Caminova DjVu Browser Plug-in 6.1.4 Build 27999 已经修复此漏洞，建议用户下载使用： https://www.caminova.net/ja/downloads/download.aspx?id=1

CNVD-2012-09650	Apache Struts 'ParameterInterceptor' Class OGNL 安全绕过漏洞	高	Apache Software Foundation Struts 2.3.1.2 已经修复此漏洞，建议用户下 载使用： http://struts.apache.org/
CNVD-2012-09704	RSA enVision 环境变量信息泄露 漏洞	高	RSA Security enVision Platform 4.1 P3 和 RSA Security enVision Platform 4.0 SP4 P5 已经修复此漏洞，建议用户下 载使用： http://www.rsa.com/node.aspx?id=3170
CNVD-2012-09637	Mindjet MindManager 2012 DLL 存在多个漏洞	高	暂无
CNVD-2012-09625	QEMU KVM 本地权限提升漏洞	高	目前官方已发布发布相关补丁和临时 解决方案，请及时安装： http://www.nongnu.org/qemu/

表 3 部分高危漏洞列表

小结：本周，Mozilla，Hitachi，Google 和 FFmpeg 的应用产品被披露存在多个安全漏洞，远程攻击者可以利用漏洞执行任意脚本代码、控制目标用户系统、获得敏感信息。此外 ComponentOne 零日漏洞相关工业控制系统 B/S 用户构成较为严重的威胁。

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 Open Enterprise Server 安全漏洞

本周，Novell 发布升级程序，修补了 Open Enterprise Server 的安全漏洞。远程攻击者可以利用漏洞执行任意代码。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=8732

本周要闻速递

1. HTC 承认部分 Android 手机 WiFi 密码泄露

据国外媒体报道，一些 HTC 的 Android 手机存在 WiFi 证书及密码被窃风险。美国计算机应急准备小组(US-CERT)的一项公告显示，HTC 的部分 Android 手机存在能够被黑客利用的漏洞，受影响的用户应该及时去 HTC 的支持网站进行软件更新。据安全研

究人员发现，HTC 旗下部分 Android 手机，带有 android.permission.ACCESS_WIFI_STATE 许可的第三方 Android 应用，可以通过利用相关命令来访问手机所使用网络的 WiFi 安全凭证。这有可能导致 WiFi 网络的相关安全信息在未经许可的情况下，被传送至其他远程服务器中。研究人员于去年 9 月发现了这一安全漏洞，并在最近正式对外公布。该漏洞主要的运行情况如下：受影响的 Android 会在该手机的应用程序中建立公开的 802.1X 密码，使之具有访问手机 Wi-Fi 状态的权限。应用程序能够获得并存储 Wi-Fi 网络的 SSID、用户名和密码的权限。如果该应用程序还具有互联网访问权限，它就可以把被盗数据发给攻击者。因此，该漏洞自身虽然没有访问 802.1X 设置的权限，但能够通过应用程序达到信息窃取的目的。HTC 和谷歌于 2011 年 9 月获知该漏洞，并已经开始着手修复该问题。

参考链接: http://sc.city.ifeng.com/technology/detail_2012_02/03/147718_0.shtml

2. Xorg 1.11 爆本地安全漏洞

Linux 桌面系统爆出了低级严重的本地安全漏洞，只要是采用 Xorg 1.11 组件的 Linux 发行版，用户可以在不需输入密码的情况下，直接利用快捷键 Ctrl+Alt+*（数字键上的*）就可以绕过屏幕锁定状态。这个漏洞只影响运行了没有打补丁的 Xorg server 1.11+组件的系统，目前涉及的发行版有 Fedora 16, Arch Linux, Fuduntu, Debian unstable 等等。而由于 Ubuntu 目前使用的 Xorg server 版本小于 1.11，所以暂时没有波及到 (Ubuntu 12.04 发布时应该会采用 Xorg 1.11，但目前还在使用 1.10.4)。

参考链接: <http://www.lupaworld.com/article-215497-1.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