

信息安全漏洞周报

2012 年 2 月 20 日-2012 年 2 月 26 日

2012 年 第8 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 107 个，其中高危漏洞 33 个、中危漏洞 74 个、低危漏洞 0 个。上述漏洞中，可利用来实施远程攻击的漏洞有 102 个。本周收录的漏洞中，已有 60 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“WebcamXP/Webcam7 目录遍历漏洞”、“DAMN Hash Calculator 远程堆缓冲区溢出漏洞”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 2 家合作伙伴单位报送了本周收录的全部 107 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，网御星云公司、上海交通大学报送了两个涉及国产网站内容管理系统、国外厂商生产的邮件系统的 XSS 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	69	0
安天实验室	29	0
绿盟科技	27	0
天融信	21	0
恒安嘉新	21	0
安氏领信	4	0
网御星云	1	1
上海交通大学	1	1
总计	107（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 SAP、Novell、Linux 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	SAP	5	4.7%
2	Novell	4	3.7%
3	Linux	4	3.7%
4	VOXTRONIC	3	2.8%
5	Cisco	3	2.8%
6	WordPress	3	2.8%
7	D-Link	3	2.8%
8	RACON Software GmbH Linz	2	1.9%
9	Typo3	2	1.9%
10	Jeskola	2	1.9%
11	其它	76	71%

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、Novell GroupWise Messenger 安全漏洞

Novell GroupWise Messenger 是一款基于 GroupWise 平台的即时交流工具。本周，上述 Novell 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或使应用程序崩溃，导致内存损坏。CNVD 收录的相关漏洞包括：Novell GroupWise Messenger 内存损坏漏洞、Novell GroupWise Messenger Client '.nmx'文件栈缓冲区溢出漏洞、Novell GroupWise Messenger 'createsearch'命令远程内存破坏漏洞、Novell GroupWise Messenger 'NM_A_PARM1'标签堆内存破坏漏洞。上述漏洞的综合评级均为“高危”。目前，Novell 尚未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=40090
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=40108
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=40128
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=40129

2、Cisco 产品安全漏洞

Cisco Small Business SRP500 系列被 ISP、VAR 或 SI 等托管电信运营商用作托管客户端设备(CPE)，服务于它们的中小型企业客户。本周，该 Cisco 产品被披露存在多个安全漏洞。远程攻击者可以利用漏洞上传恶意文件、执行任意操作系统命令或控制设备。CNVD 收录的相关漏洞包括：Cisco Small Business SRP500 系列应用目录遍历漏洞、Cisco Small Business SRP500 系列应用未授权访问安全绕过漏洞、Cisco Small Business SRP500 系列 WEB 接口命令注入漏洞。其中，“Cisco Small Business SRP500 系列 WEB 接口命令注入漏洞”的综合评级为“高危”。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=40916
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=40917
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=40918

3、D-Link 产品安全漏洞

本周，D-Link 的两款产品 DCS、DSL-2640B 被披露存在多个安全漏洞。D-Link DCS 是摄像设备；D-Link DSL-2640B 则是路由设备。攻击者可以利用上述产品漏洞执行恶意操作，运行特权命令，更改配置或导致拒绝服务。CNVD 收录的相关漏洞包括：D-Link DCS 产品'security.cgi'跨站请求伪造漏洞、D-Link DSL-2640B MAC 地址验证绕过漏洞、D-Link DSL-2640B 'redpass.cgi'跨站请求伪造漏洞。目前，互联网上已经出现针对“D-Link DCS 产品'security.cgi'跨站请求伪造漏洞”的攻击代码，但厂商尚未发布该漏洞的修补程序。厂商目前仅修补了“D-Link DSL-2640B 'redpass.cgi'跨站请求伪造漏洞”，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=40921
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=40935
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=40435

4、Linux Kernel 安全漏洞

Linux Kernel 是开源操作系统 Linux 所使用的内核。本周，Linux 内核被披露存在多个安全漏洞，攻击者可以利用漏洞发起拒绝服务攻击。CNVD 收录的相关漏洞包括：Linux Kernel epoll Subsystem 'eventpoll.c'本地拒绝服务漏洞、Linux Kernel 'Clone()'函数'CLONE_IO'标记拒绝服务漏洞、Linux Kernel m_start 本地拒绝服务漏洞。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=40940
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=40936
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=40172

5、WebcamXP/Webcam7 目录遍历漏洞

WebcamXP/Webcam7 是一款网络摄像软件。本周，WebcamXP/Webcam7 产品被披露存在一个目录遍历漏洞。由于应用程序的 WEB 接口未能正确过滤用户提交的请求，攻击者可以提交目录遍历序列请求，以应用程序上下文查看系统文件内容。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 Moonware Studios webcamXP 5.5.1.2 版本和 webcam 7 0.9.9.32 版本。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=40755

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-2012-10165	phpDenora 'ed'参数 SQL 注入漏洞	高	暂无
CNVD-2012-10161	snom VoIP 电话固件远程特权提升漏洞	高	暂无
CNVD-2012-10149	Csound 'getnum()'缓冲区溢出漏洞 (CNVD-2012-10149)	高	Csound 5.16.6 已经修复此漏洞，建议用户下载使用： http://sourceforge.net/projects/csound/files/csound5/csound5.16/Version 5.16_Notes/view
CNVD-2012-10163	YVS Image Gallery 'album_id' SQL 注入漏洞	高	暂无
CNVD-2012-10133	Unity Web Player 堆内存破坏漏洞	高	暂无
CNVD-2012-10124	Net4Switch ipswcom ActiveX 控件缓冲区溢出漏洞	高	暂无
CNVD-2012-10137	Joomla! X-Shop 组件'idd'参数 SQL 注入漏洞	高	暂无
CNVD-2012-10106	Jeskola Buzz 内存破坏漏洞	高	暂无
CNVD-2012-10054	7T AQUIS DLL 装载任意代码执行漏洞	高	用户可参考如下供应商提供的补丁程序： http://aquis.s3.amazonaws.com/AQUIS_1.5_14-12-2011.exe
CNVD-2012-10061	PHP 'filter_globals'结构任意代码执行漏洞	高	PHP 5.3 已经修复此漏洞，建议用户下载使用： http://www.php.net/

表 3 部分高危漏洞列表

小结：本周，Novell GroupWise Messenger 被披露存在多个综合评级为“高危”的安全漏洞，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或使应用程序崩溃，导致内存损坏。且这些漏洞尚未被厂商修补。Cisco 应用程序，D-Link 网络设备和 Linux 操作系统也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，WebcamXP/Webcam7 摄像软件零日漏洞以及多个 Web 应用软件的高危漏洞需引起相关企业和终端用户注意，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、IBM 发布升级程序，修补 WebSphere Lombardi Edition 安全漏洞

本周，IBM 发布升级程序，修补了 WebSphere Lombardi Edition 存在的安全漏洞，避免远程攻击者可以获得敏感信息或劫持用户会话。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=10755

本周要闻速递

1. iOS 5 允许非法远程访问相册

据国外媒体报道，到目前为止对于 iOS 5 没有安全漏洞需要修补，但最近新发现的一个漏洞比较危险，iPhone 4 是唯一受该漏洞影响的苹果设备。由 iPatch 开展的测试发现，如果用户瞬间拆除 iPhone 4 中的电池，用户可以在不使用 SIM 卡重启的情况下访问相册。iPhone 4 从照相机应用中启动相册，用户能够从处于密码锁定状态的设备中访问该相册。当电池被拆除的时候，手机可能会遗忘一些安全措施设置。

参考链接：http://itpx.eol.cn/hydt_10909/20120227/t20120227_744945.shtml

2. Android 被曝存在安全漏洞

在 Google Android 智能手机操作系统中，网络安全专家发现一个组件漏洞，专家称漏洞会导致黑客控制设备。安全专家还表示，移动设备招致的攻击范围扩大，比 PC 还要大。黑客能找到之前未知的软件缺陷，然后利用漏洞，通过感染性链接、附件传送恶意软件。智能手机用户要对此类攻击作好防备，因为这种攻击无法确定身份，能穿过移动设备安全软件。之前，也有研究人员指出智能手机系统存在漏洞。2009 年 7 月，研究人员找到攻击苹果 iPhone 的方法，它可以在短信中发送恶意代码，手机用户看不见。数周后，苹果修改了软件漏洞。据报道，漏洞适用于 Andorid2.2 系统。目前大约 28% 的 Android 设备安装该版软件。

参考链接: <http://info.tele.hc360.com/2012/02/270850376718.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