

信息安全漏洞周报

2013 年 2 月 04 日-2012 年 2 月 17 日

2013 年第 6、7 期合刊

本周漏洞基本情况

2 月 4 日至 2 月 17 日期间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 212 个，其中高危漏洞 73 个、中危漏洞 124 个、低危漏洞 15 个。上述漏洞中，可利用来实施远程攻击的漏洞有 165 个。本周收录的漏洞中，已有 170 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“xNBD '/tmp/xnbd.log'不安全临时文件创建漏洞”、“D-Link DIR-300 存在多个 HTML 注入漏洞”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 家成员单位向 CNVD 报送了 2 月 4 日至 2 月 17 日收录的全部 212 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技等单位报送数量较多。此外，High-Tech Bridge Security Research Lab 和个人报送者向 CNVD 提交了 11 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	361	0
绿盟科技	100	0
天融信	50	0
安天实验室	66	0
恒安嘉新	9	0
High-Tech Bridge Security Research L	4	4
个人	7	7
报送总计	597	11
录入总计	212（去重）	11

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、Oracle、Cisco、WordPress 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	53	11%
2	Oracle	52	7%
3	Cisco	10	7%
4	WordPress	7	7%
5	D-Link	6	5%
6	Nagios	6	4%
7	HP	5	3%
8	IBM	3	3%
9	RedHat	3	2%
10	Joomla!	3	1%
11	其它	64	50%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 212 个漏洞。其中应用程序漏洞 136 个，WEB 应用漏洞 23 个，操作系统漏洞 39 个，网络设备漏洞 14 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	136
WEB 应用漏洞	23
网络设备漏洞	14
操作系统漏洞	39
数据库漏洞	0
安全产品漏洞	0

表 3 漏洞按影响类型统计表

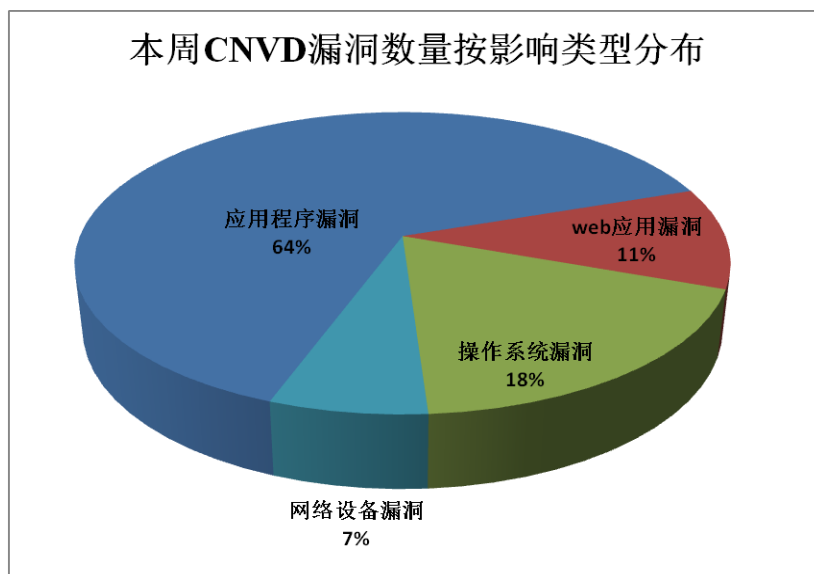


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 14 个网络设备漏洞：Cisco IOS Catalyst Switches HTTP Server 拒绝服务漏洞、D-Link DIR-300 存在多个 HTML 注入漏洞、Lorex LNC116/LNC104 IP Camera 远程验证绕过漏洞、Cisco Linksys E1500/E2500 操作系统命令注入漏洞、Cisco Linksys E1500 Router 'next_page' 目录遍历漏洞、Cisco Linksys E1500 Router 更改密码安全绕过漏洞、Cisco Linksys E1500 Router 跨站请求伪造漏洞、Cisco Linksys E1500 Router 跨站脚本漏洞、Cisco Linksys E1500 Router 重定向漏洞、D-Link DIR-600 和 DIR-300 远程命令执行漏洞、D-Link DIR-600 和 DIR-300 存在多个信息泄露漏洞、D-Link DIR-600 和 DIR-300 密码加密漏洞、D-Link DIR-600 和 DIR-300 安全绕过漏洞、D-Link DIR-600 和 DIR-300 跨站脚本漏洞。

其中，“D-Link DIR-600 和 DIR-300 远程命令执行漏洞”的综合评级为“高危”。目前，互联网上已经出现了针对 D-Link、Cisco、Lorex 等相关厂商产品的攻击代码，相关厂商已经发布了漏洞的修补程序。

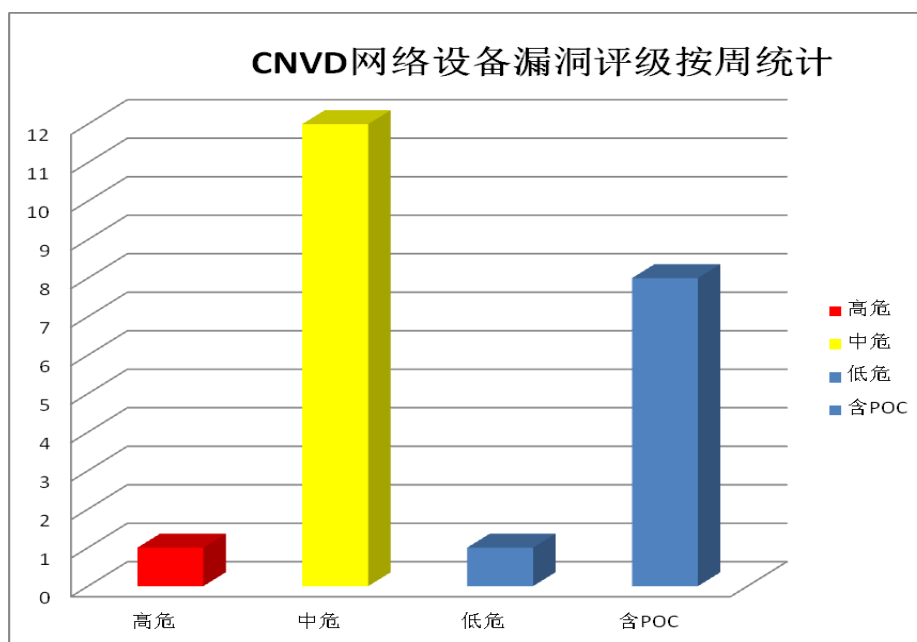


图 2 网络设备漏洞统计

本周重要漏洞信息

2月4日至2月17日，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13日，微软发布了2013年2月份的月度例行安全公告，共含12项更新，修复了Windows内核、.NET Framework、Server 软件(SharePoint Server, FAST Search Server)，Internet Explorer 浏览器中存在的多个安全漏洞。其中，5项更新的综合评级为“严重”级别（微软定义的威胁最高级别），其余7项更新综合评级均为“重要”级别。利用上述漏洞，攻击者可以远程执行代码，提升特权或进行拒绝服务攻击。

CNVD收录的相关漏洞包括：Microsoft Internet Explorer InsertElem 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer Shift JIS Character 信息泄露漏洞、Microsoft Internet Explorer vtable 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer CDispNode 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer CHTML 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer CMarkup 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer CObjectElem 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer COMWindowProxy 内存错误引用远程代码执行漏洞等。上述漏洞的综合评级均为“高危”。目前，厂商已发布了上述漏洞的修补程序，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=CNVD-2013-19922

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19926

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19929

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19916

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19917

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19918

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19919

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19920

2、Cisco 产品安全漏洞

Cisco Linksys E1500 Router 是一款无线路由器设备；Cisco IOS Catalyst Switches 是思科公司开发的交换机设备，Cisco IOS 是设备的操作系统；Cisco Unity EXPress 提供了专为中小型机构环境设计的语音邮件和自动接听服务。本周，上述思科产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息或劫持用户会话，导致设备崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Cisco Linksys E1500 Router 跨站脚本漏洞、Cisco Linksys E1500 Router 跨站请求伪造漏洞、Cisco Linksys E1500 Router 更改密码安全绕过漏洞、Cisco Linksys E1500 Router 'next_page'目录遍历漏洞、Cisco Linksys E1500/E2500 操作系统命令注入漏洞、Cisco IOS Catalyst Switches HTTP Server 拒绝服务漏洞等。目前，厂商已发布了“Cisco IOS Catalyst Switches HTTP Server 拒绝服务漏洞”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=CNVD-2013-19972

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19971

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19970

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19969

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19968

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19911

3、Oracle 产品安全漏洞

Oracle Java Runtime Environment 主要为 JAVA 应用程序提供运行环境，该产品被披露存在多个安全漏洞。

CNVD 收录的相关漏洞包括：Oracle Java SE 存在未明漏洞（CNVD-2013-19779、CNVD-2013-19781、CNVD-2013-19782、CNVD-2013-19783、CNVD-2013-19784、CNVD-2013-19785、CNVD-2013-19786、CNVD-2013-19787）等。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=CNVD-2013-19779
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19781
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19782
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19783
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19784
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19785
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19786
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19787

4、Nagios 安全漏洞

Nagios 是一款免费开源的主机和服务监视软件。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息或劫持用户会话，发起拒绝服务攻击，执行任意代码。

CNVD 收录的相关漏洞包括：Nagios QL 跨站请求伪造漏洞、Nagios QL 跨站请求伪造漏洞、Nagios QL 跨站脚本漏洞、Nagios 配置文件注入漏洞、Nagios Autodiscovery SQL 注入漏洞、Nagios Autodiscovery 任意代码执行漏洞。其中，“Nagios Autodiscovery SQL 注入漏洞”和“Nagios Autodiscovery 任意代码执行漏洞”的综合评级均为“高危”。厂商尚未发布该漏洞的修补程序，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=CNVD-2013-19847
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19843
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19844
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19846
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19848
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19845

5、D-Link DIR-300 存在多个 HTML 注入漏洞

D-Link DIR-300 是一款无线路由器设备。本周，D-Link DIR-300 被披露存在多个 HTML 注入漏洞。远程攻击者利用漏洞可进行 HTML 注入攻击，获得敏感信息或劫持用户会话。目前，互联网上已经出现针对该漏洞的攻击代码，厂商尚未发布该漏洞的修补程序，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=CNVD-2013-19908

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-2013-19973	D-Link DIR-600 和 DIR-300 远程命令执行漏洞	高	暂无
CNVD-2013-19865	Android PowerVR SGX 驱动敏感信息泄露漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： http://code.google.com/p/android/issues/detail?id=21523
CNVD-2013-19863	AdaptCMS 'question' POST 参数 SQL 注入漏洞	高	暂无
CNVD-2013-19875	Glossword 'login.php' SQL 注入漏洞	高	暂无
CNVD-2013-19893	Opera Web Browser Use-After-Free 内存破坏漏洞	高	暂无
CNVD-2013-19718	MiniUPnP MiniUPnPd 空指针引用漏洞	高	MiniUPnP 1.1 已经修复此漏洞，建议用户下载使用： http://miniupnp.free.fr/
CNVD-2013-19770	pGB SQL 注入漏洞	高	暂无
CNVD-2013-19836	Free Monthly Websites 任意文件上传漏洞	高	暂无
CNVD-2013-19720	Pale Moon libpixmap 栈缓冲区溢出漏洞	高	Pale Moon 15.4 已经修复此漏洞，建议用户下载使用： http://www.palemoon.org/releasesnotes-ng.shtml
CNVD-2013-19841	latd 缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

小结：2 月 13 日，微软发布了 2013 年 2 月份的月度例行安全公告，共含 12 项更新，修复了 Windows 内核、.NET Framework、Server 软件（SharePoint Server，FAST Search Server）以及 Internet Explorer 浏览器中存在的多个安全漏洞，服务器和桌面操作系统用户需及时进行更新。本周，Nagios、Cisco 多款产品被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息或劫持用户会话，执行任意代码。Oracle Java Runtime Environment 也被披露存在多个漏洞。此外，D-Link DIR-300 被披露存在零日漏洞，相关用户应随时关注厂商主页，及时获取修复补丁或解决方案。

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、Red Hat 发布升级程序，修补 Enterprise Virtualization Manager 漏洞

Red Hat Enterprise Virtualization Manager 是一款红帽子推出的企业虚拟化管理应用解决方案。本周，Red Hat 修补了 Enterprise Virtualization Manager 存在的漏洞。攻击者可以利用漏洞获取敏感信息或进行拒绝服务攻击。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=31576
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=31577

本周要闻速递

1. iOS 6.1.2 将在 2 月 20 日发布 修复锁屏漏洞

上周，苹果发报告称预期下周会推出 iOS 6 的更新版本，同时将解决锁屏密码被绕过的危险漏洞。德国博客 iFun 近日表示 iOS 6.1.2 将在下周初推出，最有可能是 2 月 20 日抵达。当地时间上周三，苹果 iOS 6.1 被爆出锁屏漏洞，攻击者利用漏洞可以通过拨打 112 的操作绕过锁屏 PIN 来读取用户数据，包括联系人、语音邮件、照片等，但不能切入 iOS 主屏。

参考链接：<http://tech.hexun.com/2013-02-18/151192363.html>

2. 开发者爆谷歌商店安全漏洞 用户信息被轻易泄露

2 月 17 日消息，据国外媒体报道，澳大利亚一名应用开发者日前称，谷歌应用商店涉嫌向开发者泄露用户私人信息，给后者财产等安全构成威胁。当用户购买付费应用时，谷歌商店会自动将用户的姓名、地址、邮箱等私人信息发送给开发者。进一步利用这些信息，可套取用户的银行账号等信息，也可以借机入侵用户的手机。目前尚不清楚，下载免费应用的用户信息是否不会泄露。

参考链接：<http://www.techweb.com.cn/world/2013-02-17/1277028.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