

信息安全漏洞周报

2013 年 02 月 18 日-2013 年 02 月 24 日

2013 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**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 279 个，其中高危漏洞 93 个、中危漏洞 149 个、低危漏洞 37 个。上述漏洞中，可利用来实施远程攻击的漏洞有 249 个。本周收录的漏洞中，已有 197 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“Dell SonicWALL Scrutinizer SQL 注入漏洞”、“Linksys WAG200G 命令注入漏洞”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 6 家成员单位和多个合作伙伴报送了本周收录的全部 279 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、天融信、安天实验室等单位报送数量较多。此外，上海交通大学和 High-Tech Bridge Security Research Lab 向 CNVD 提交了 2 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	179	0
启明星辰	146	0
天融信	76	0
安天实验室	44	0
恒安嘉新	6	0
东软	19	0
High-Tech Bridge Security Research L	1	1
上海交通大学	1	1

报送总计	472	2
录入总计	279（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 Adobe、IBM、Mozilla、Linux 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	Adobe	24	9%
2	IBM	23	8%
3	Mozilla	14	5%
4	Linux	11	4%
5	Cisco	10	4%
6	Drupal	8	3%
7	FFmpeg	8	3%
8	SAP	5	2%
9	Oracle	5	2%
10	HP	4	1%
11	其它	167	59%

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 279 个漏洞。其中应用程序漏洞 165 个，WEB 应用漏洞 70 个，操作系统漏洞 16 个，网络设备漏洞 26 个，数据库漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	165
WEB 应用漏洞	70
网络设备漏洞	26
数据库漏洞	2
操作系统漏洞	16

表 3 漏洞按影响类型统计表

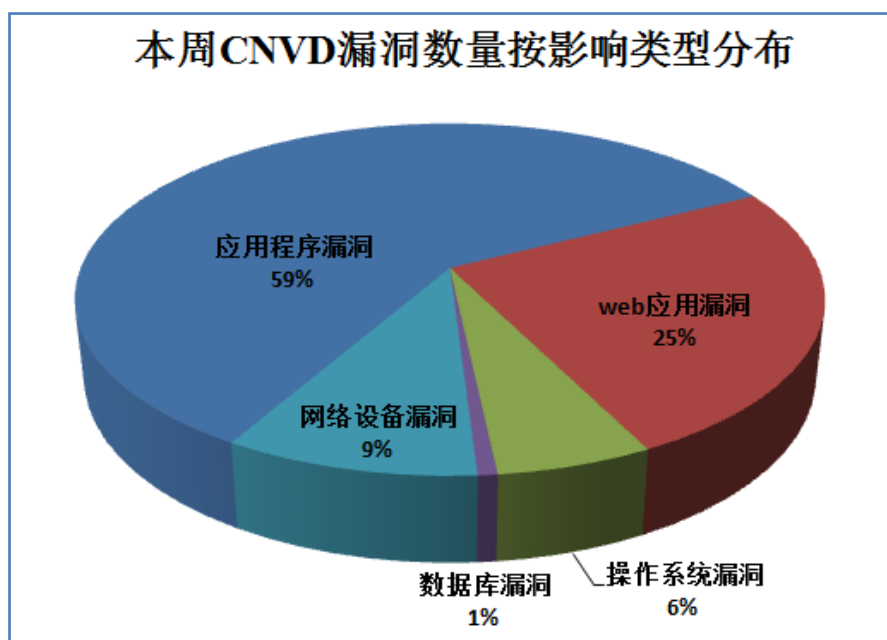


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 Buffalo、Cisco、NetGear、TP-LINK、Edimax 等多个厂商产品的 26 个网络设备漏洞，例如：Buffalo TeraStation Network Attached Storage (NAS) TS-Series 文件包含漏洞、Cisco Small Business Wireless Access Points 拒绝服务漏洞、NetGear DGN1000B 无线路由器存在多个漏洞、TP-LINK TL-WR2543ND 管理面板存在多个跨站请求伪造漏洞、Edimax EW-7206APg 和 EW-7209APg 开放重定向漏洞、NetGear DGN2200B 无线路由器命令注入漏洞等。

目前，互联网上已经出现了针对相关厂商产品的攻击代码，厂商已经发布了漏洞的修补程序。

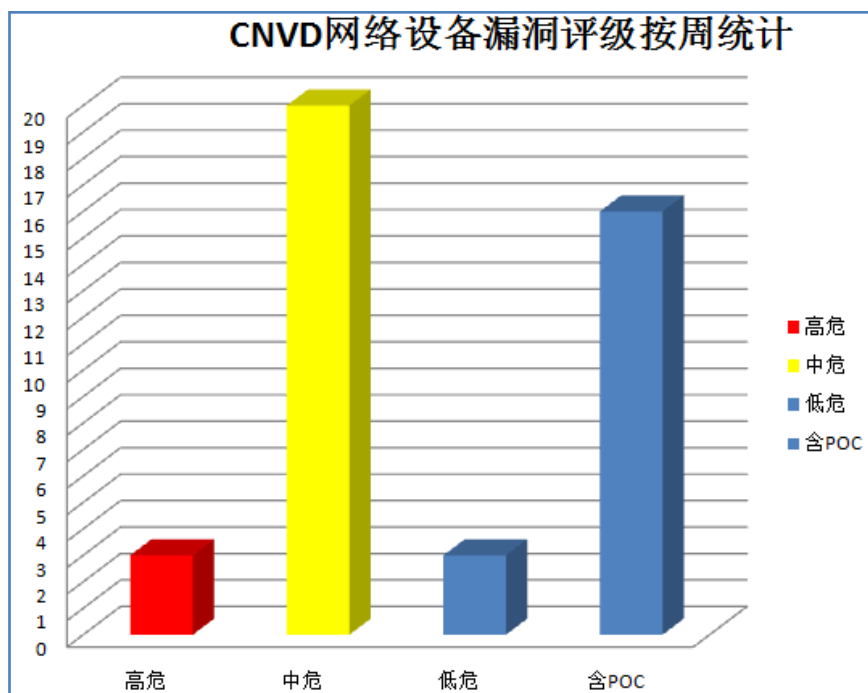


图 2 网络设备漏洞统计

本周重要漏洞信息

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，攻击者利用漏洞可构建恶意 WEB 页，诱使用户解析，执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird/SeaMonkey nsSaveAsCharset::DoCharsetConversion 缓冲区溢出漏洞、Mozilla Firefox/Thunderbird/SeaMonkey nsCodingStateMachine::NextState 越界读漏洞、Mozilla Firefox/Thunderbird/SeaMonkey nsOverflowContinuationTracker::Finish 内存错误引用漏洞、Mozilla Firefox/Thunderbird/SeaMonkey ClusterIterator::NextCluster 越界读漏洞、Mozilla Firefox/Thunderbird/SeaMonkey nsImageLoadingContent::OnStopContainer 内存错误引用漏洞、Mozilla Firefox/Thunderbird/SeaMonkey nsDisplayBoxShadowOuter::Paint 内存错误引用漏洞、Mozilla Firefox/Thunderbird/SeaMonkey nsPrintEngine::CommonPrint 内存错误引用漏洞、Mozilla Firefox/Thunderbird/SeaMonkey 安全限制绕过漏洞等。上述漏洞的综合评级均为“高危”。厂商已发布了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-2013-20201
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20199
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20200
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20198
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20194
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20186
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20187
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20185

2、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player/AIR 缓冲区溢出漏洞（CNVD-2013-20060）、Adobe Flash Player/AIR 缓冲区溢出漏洞（CNVD-2013-20061）、Adobe Flash Player/AIR 缓冲区溢出漏洞（CNVD-2013-20062）、Adobe Flash Player/AIR 缓冲区溢出漏洞（CNVD-2013-20063）、Adobe Flash Player/AIR 缓冲区溢出漏洞（CNVD-2013-20064）、Adobe Flash Player/AIR 缓冲区溢出漏洞（CNVD-2013-20066）、Adobe Flash Player/AIR 缓冲区溢出漏洞（CNVD-2013-20067）、Adobe Flash Player/AIR 缓冲区溢出漏洞（CNVD-2013-20068）等。上述漏洞的综合评级均为“高危”。厂商已发布了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-2013-20060
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20061
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20062
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20063
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20064
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20066
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20067
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20068

3、Oracle 产品安全漏洞

Oracle Java Runtime Environment 是一款为 JAVA 应用程序提供可靠的运行环境的解决方案。本周，上述 Oracle 产品被披露存在多个安全漏洞，攻击者利用漏洞可构建特制的 Java 程序诱使用户加载（通常通过垃圾邮件或挂马的方式），严重的可取得用户主机的控制权。

CNVD 收录的相关漏洞包括：Oracle Java SE 远程漏洞（CNVD-2013-20170、

CNVD-2013-20172、CNVD-2013-20174、CNVD-2013-20171)、Oracle Java SE Deployment 子组件远程 JRE 漏洞。其中，除“Oracle Java SE 远程漏洞（CNVD-2013-20171）”外，其余漏洞的综合评级均为“高危”。厂商已发布了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-2013-20170

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20172

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20174

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20038

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20171

4、Linux kernel 安全漏洞

Linux kernel 是 Linux 操作系统内核。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞发起拒绝服务攻击，导致系统崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Linux Kernel 'setsockopt()'空指针引用拒绝服务漏洞、Linux Kernel 'pmd_present'拒绝服务漏洞、Linux Kernel 拒绝服务漏洞（CNVD-2013-20228）、Linux 内核 PTRACE_SETREGS 竞争条件漏洞、Linux 内核拒绝服务漏洞、Linux Kernel 本地权限提升漏洞、Linux Kernel 'MSR'驱动本地权限提升漏洞、Linux Kernel '__skb_recv_datagram()'本地拒绝服务漏洞等。厂商已发布了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-2013-20227

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20226

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20228

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20122

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20158

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20100

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20023

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19992

5、Dell SonicWALL Scrutinizer SQL 注入漏洞

Dell SonicWALL Scrutinizer 是一款网络通信监视和日志分析程序。本周，该产品被披露存在一个综合评级为“高危”的 SQL 注入漏洞。由于 Dell SonicWALL Scrutinizer fa_web.cgi 文件中的 gadget listing 模块对 orderby 或 gadget 参数缺少过滤，攻击者利用漏洞可进行 SQL 注入攻击，获得数据库敏感信息。目前，互联网上已经出现了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-2013-20084

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-2013-20229	TYPO3 CoolURI 存在未明 SQL 注入漏洞	高	TYPO3 CoolURI extension 1.0.30 已经修复此漏洞, 建议用户下载使用: http://typo3.org/extensions/repository/view/cooluri/1.0.14/
CNVD-2013-20225	CoDeSys 'Gateway Server'栈缓冲区溢出漏洞	高	3S CoDeSys 2.3.9.38 已经修复此漏洞, 建议用户下载使用: http://www.3s-software.com/index.shtml?codesys_dev_dir
CNVD-2013-20167	Scripts Genie DomainTrader Script 'id' SQL 注入漏洞	高	暂无
CNVD-2013-20233	WordPress Mingle Forum 插件 SQL 注入漏洞	高	WordPress Mingle Forum Plugin 1.0.33.4 已经修复此漏洞, 建议用户下载使用: http://wordpress.org/extend/plugins/mingle-forum/
CNVD-2013-20136	Pidgin 'Libpurple' HTTP 头栈缓冲区溢出漏洞	高	Pidgin 2.10.7 已经修复此漏洞, 建议用户下载使用: http://www.pidgin.im/
CNVD-2013-20160	NetGear DGN2200B 无线路由器命令注入漏洞	高	暂无
CNVD-2013-20143	SAP NetWeaver 'msg_server.exe'远程代码执行漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息: https://service.sap.com/sap/support/notes/1800603
CNVD-2013-20164	ECShop 支持宝插件 SQL 注入漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息: http://bbs.ecshop.com/viewthread.php?tid=1125380
CNVD-2013-20165	Kodak InSite 'EmailPassword.asp' SQL 注入漏洞	高	暂无
CNVD-2013-20140	Ruby nori Gem 'XML'参数任意命令执行漏洞	高	nori gem for Ruby 2.0.3 已经修复此漏洞, 建议用户下载使用: https://github.com/savonrb/nori/blob/master/CHANGELOG.md

表 3 部分高危漏洞列表

小结：Adobe Flash Player、Oracle Java Runtime Environment 和 Mozilla 的多款产品被披露存在多个漏洞，有可能诱发大规模的网页挂马或垃圾邮件攻击。Linux kernel 也被披露存在多个漏洞，攻击者利用漏洞可发起拒绝服务攻击，对服务器应用主机构成较为严重的威胁。Dell SonicWALL Scrutinizer 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。此外，本周在国内应用广泛的 EcShop 电子商务建站软件被披露存在高危漏洞，目前厂商已经发布了补丁，相关用户应及时下载理更新。

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、Symantec 发布升级程序，修补 Encryption Desktop 漏洞

Symantec Encryption Desktop 是一款桌面加密软件。本周，Symantec 修补了 Encryption Desktop 存在的漏洞。攻击者可以利用漏洞导致缓冲区溢出或提升权限。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=32017
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=32014

本周要闻速递

1. HTC 承诺修复手机漏洞

据国外媒体报道，HTC 美国与美国联邦贸易委员会(FTC)就该品牌智能手机所存在的用户安全信息隐患以及安全漏洞指控达成有条件和解，并保证将尽快改善手机的安全性能。据了解，早些时候 FTC 指出 HTC 手机当中存在多个不同程度的安全漏洞，这些漏洞涉及 Carriers IQ 和 HTC Loggers 两款软件，其能够允许第三方恶意软件绕过 Android 操作系统的安全检测机制，从而对诸如地理位置信息和短信内容等用户敏感信息造成泄露危害。目前，FTC 已经要求 HTC 尽快建立全面的手机安全解决方案，而且也要联合运营商及时向用户分发最新的安全修正补丁。同时，HTC 也因此被勒令必须要在今后的 20 年里接受单独的安全评估。

参考链接：<http://henan.sina.com.cn/shuma/shouji/2013-02-25/268-27568.html>

2. 美国试行指纹支付系统 隐私安全仍存有漏洞

据中国之声《央广新闻》报道，未来学家曾预测纸币和信用卡将会消失，指纹和视网膜扫描仪将会完成许多身份认证问题完成日常事物，比如买东西。据美国媒体 22 日

报道，一项最新技术的指纹支付系统已经在美国南卡州试行。这个指纹支付系统是由美国 Nexus 公司生产。使用者首先是得到了个人的银行户口，然后采集个人信息，银行的信息以及食指的指纹，在支付器上输入到自己的出生年月，然后刷食指，几秒钟之后，机器就识别了他的指纹，同时根据指纹上脉搏的迹象，完成这次交易。目前指纹识别系统的技术存在着指纹被冒用的风险，而业内就观察，指纹技术自身带来了个人隐私泄漏的隐患，但是脉搏的检测无疑是一个正确的方向，再安全的措施都会有漏洞，会遭到一些威胁，问题就在于如何让受到的威胁程度降到最低。

参考链接：http://news.china.com.cn/live/2013-02/25/content_18787898.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