

信息安全漏洞周报

2013 年 11 月 25 日-2013 年 12 月 01 日

2013 年第 48 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 153 个，其中高危漏洞 44 个、中危漏洞 87 个、低危漏洞 22 个。上述漏洞中，可利用来实施远程攻击的漏洞有 131 个。本周收录的漏洞中，已有 128 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“Thomson Reuters Velocity Analytics 恶意 URL 远程代码注入漏洞”、“WordPress Suco Themes 'themify-ajax.php'任意文件上传漏洞”等零日攻击代码，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 4 家成员单位、国家互联网应急中心及个人报送了本周收录的全部 153 个漏洞。报送情况如表 1 所示。其中，安天实验室、启明星辰、天融信等单位报送数量较多。此外，国家互联网应急中心及个人报送者向 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
安天实验室	150	0
启明星辰	115	0
天融信	95	0
恒安嘉新	10	0
国家互联网应急中心	4	4
个人	7	7
报送总计	381	11

录入总计	153（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 FFmpeg、Drupal、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	FFmpeg	29	19%
2	Drupal	11	7%
3	Linux	7	5%
4	IBM	6	4%
5	Cisco	6	4%
6	WordPress	5	3%
7	Apache	4	3%
8	ABB	4	3%
9	Microsoft	1	1%
10	其它	80	51%

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 153 个漏洞。其中应用程序漏洞 111 个，WEB 应用漏洞 23 个，操作系统漏洞 9 个，网络设备漏洞 10 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	111
WEB 应用漏洞	23
网络设备漏洞	10
操作系统漏洞	9

表 3 漏洞按影响类型统计表

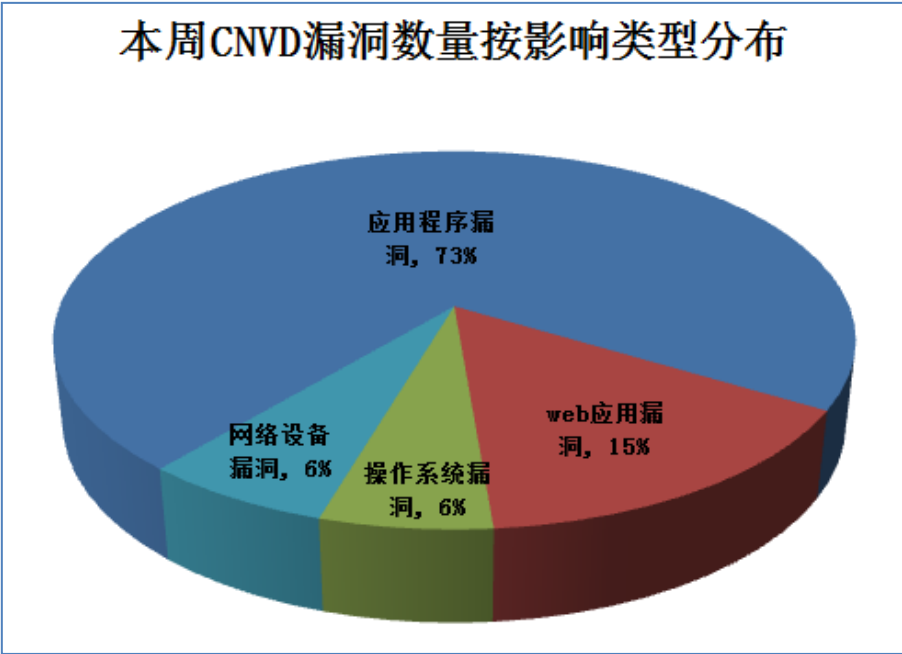


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 11 个电信行业漏洞和 4 个工控系统漏洞（如下列表所示）。其中，“D-Link DES-3800 系列 WEB 管理实现远程拒绝服务漏洞、ABB Test Signal Viewer CWGraph3D ActiveX 控件远程代码执行漏洞、ABB MicroSCADA 栈破坏远程代码执行漏洞、ABB RobotWare CWGraph3D ActiveX 控件远程代码执行漏洞、ABB MicroSCADA 'wserver.exe'远程代码执行漏洞”的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-14724	TP-LINK TL-WR740N/TL-WR740ND 'WlanSecurityRpm.htm'跨站请求伪造漏洞	低	否
电信	CNVD-2013-14741	ADB Discus DRG A125G 'wlbasic.html'密码信息泄露漏洞	中	否
电信	CNVD-2013-14742	ADB Discus DRG A125G 存在多个跨站请求伪造漏洞	低	否
电信	CNVD-2013-14706	D-Link DES-3800 系列 WEB 管理实现远程拒绝服务漏洞	高	是
电信	CNVD-2013-14707	D-Link DES-3800 系列 SSH 实现远程拒绝服务漏洞	中	是
电信	CNVD-2013-14708	Cisco Wireless LAN	中	是

		Controller(WLC)点击劫持漏洞		
电信	CNVD-2013-14704	Cisco Wireless LAN Controller (WLC) CAPWAP 消息处理拒绝服务漏洞	中	是
电信	CNVD-2013-14709	Cisco IOS IPSec MTU 远程拒绝服务漏洞	中	是
电信	CNVD-2013-14669	HP 2620 交换机'html/json.html' 跨站请求伪造漏洞	中	否
电信	CNVD-2013-14683	Cisco IOS MLDP 远程拒绝服务漏洞	中	是
电信	CNVD-2013-14682	Cisco IOS XE AAA DHCP 远程拒绝服务漏洞	中	是
工控系统	CNVD-2013-14743	ABB Test Signal Viewer CWGraph3D ActiveX 控件远程代码执行漏洞	高	是
工控系统	CNVD-2013-14745	ABB MicroSCADA 栈破坏远程代码执行漏洞	高	是
工控系统	CNVD-2013-14744	ABB RobotWare CWGraph3D ActiveX 控件远程代码执行漏洞	高	是
工控系统	CNVD-2013-14746	ABB MicroSCADA 'wserver.exe'远程代码执行漏洞	高	是

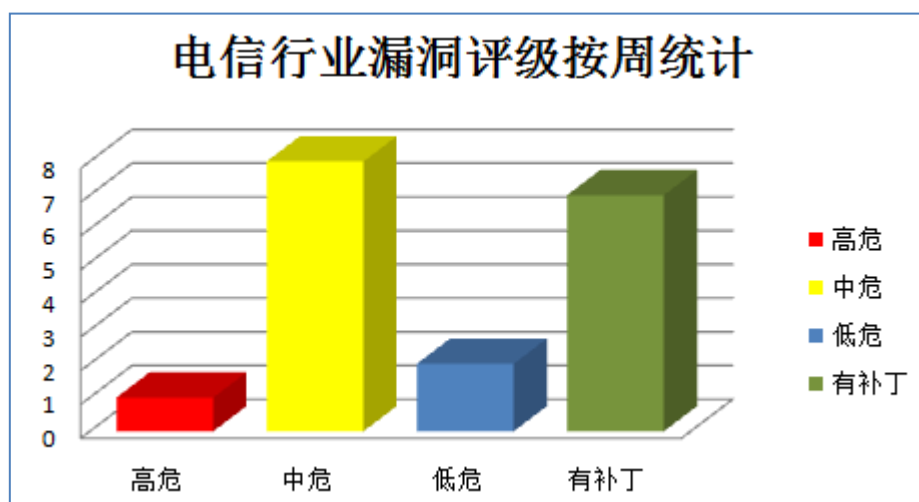


图 1 电信行业漏洞统计

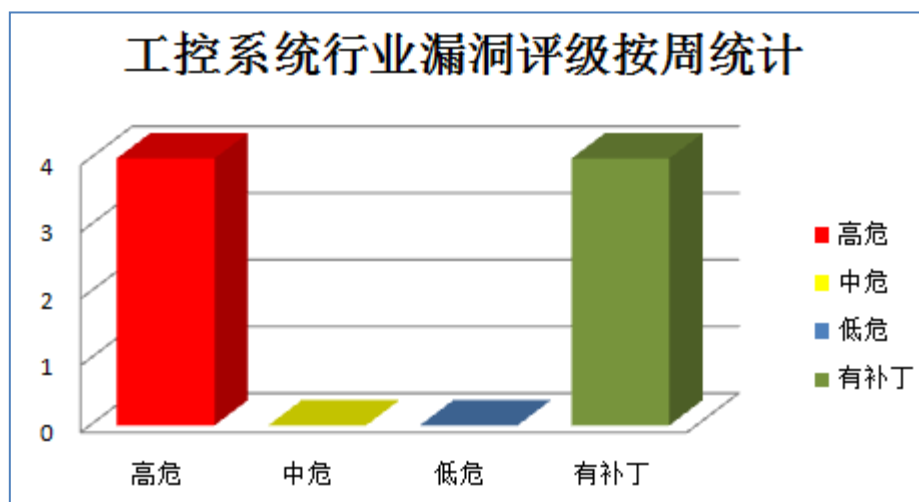


图 2 工控系统行业漏洞统计

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、Apache 产品安全漏洞

Apache Roller 是一款多用户的群组 Blog 服务器；Apache Solr 是一个开源的搜索服务器；Apache Subversion 是一款开源控制系统。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可使进程崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Apache Roller OGNL 表达式注入远程代码执行漏洞、Apache Solr 'SolrResourceLoader'目录遍历漏洞、Apache Subversion mod_dontdothat 路径匹配安全绕过漏洞、Apache Subversion 'mod_dav_svn'特制请求处理 httpd 进程拒绝服务漏洞。其中，“Apache Roller OGNL 表达式注入远程代码执行漏洞”的综合评级为“高危”。厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14766>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14747>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14752>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14791>

2、ABB 产品安全漏洞

ABB MicroSCADA 是用于变电站控制的自动化软件；RobotWare DieCast 是一款专为简化编程而开发的软件产品，用于配套 ABB 上下料与后处理机器人的操作；ABB Test Signal Viewer 是软件通知器。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：ABB Test Signal Viewer CWGraph3D ActiveX 控件远

程代码执行漏洞、ABB RobotWare CWGraph3D ActiveX 控件远程代码执行漏洞、ABB MicroSCADA 栈破坏远程代码执行漏洞、ABB MicroSCADA 'wserver.exe'远程代码执行漏洞。上述漏洞的综合评级均为“高危”。厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14743>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14744>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14745>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14746>

3、IBM 产品安全漏洞

IBM QRadar 通过监控及关联日志和流量来识别异常行为，可把散布于整个网路上、数以千计的装置端点与应用程式中的日志来源事件资料加以合并；IBM InfoSphere™ Master Data Management Server 是 IBM 提供的一种操作 MDM 解决方案；IBM Sterling Order Management 支持用户与供应商协作并优化复杂的订单执行流程；IBM Rational Performance Tester 是一种用来验证 Web 和服务器应用程序可扩展性的性能测试解决方案。本周，上述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，劫持用户会话。

CNVD 收录的相关漏洞包括：IBM QRadar Security Information and Event Manager 远程安全绕过漏洞、IBM QRadar Security Information and Event Manager 存在未明跨站脚本漏洞、IBM QRadar Security Information and Event Manager IP 信息跨站脚本漏洞、IBM InfoSphere Master Data Management Collaboration Server 跨站脚本漏洞、IBM Sterling Order Management 跨站脚本漏洞、IBM Rational Performance Tester 文件访问信息泄露漏洞。其中，“IBM QRadar Security Information and Event Manager 远程安全绕过漏洞”的综合评级为“高危”。厂商已经发布了上述漏洞的修补程序。CNVD 提醒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/flaw/show/CNVD-2013-14760>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14761>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14762>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14739>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14690>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14668>

4、Cisco 产品安全漏洞

Cisco IOS 是多数思科系统路由器和网络交换机上使用的互连网络操作系统；Cisco Wireless LAN Controller 负责全系统的无线 LAN 功能；Cisco Prime Network Registrar 是一款集成、可扩展的可靠域名系统(DNS)、动态主机配置协议(DHCP)和适用于 IPv4 和 IPv6 的 IP 地址管理(IPAM)服务的解决方案。本周，上述产品被披露存在多个漏洞，攻

击者利用漏洞可绕过获得敏感信息，使设备重载，导致拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IOS MLDP 远程拒绝服务漏洞、Cisco IOS XE AAA DHCP 远程拒绝服务漏洞、Cisco IOS IPSec MTU 远程拒绝服务漏洞、Cisco Wireless LAN Controller(WLC)点击劫持漏洞、Cisco Wireless LAN Controller (WLC) CAPWAP 消息处理拒绝服务漏洞、Cisco Prime Network Registrar Web 接口跨站脚本漏洞。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/flaw/show/CNVD-2013-14683>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14682>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14709>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14708>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14704>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14790>

5、Thomson Reuters Velocity Analytics 恶意 URL 远程代码注入漏洞

Thomson Reuters Velocity Analytics 是一款智能信息分析解决方案。本周，Thomson Reuters Velocity Analytics Vhayu Analytic Server 6.94 build 2995 及之前版本被披露存在一个代码注入漏洞，远程未验证攻击者可提交特制的 URL，利用漏洞上传恶意文件或者执行任意代码。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/flaw/show/CNVD-2013-14717>

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/flaw/list.htm>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2013-14770	Monitorix HTTP Server 远程命令执行漏洞	高	用户可联系供应商获得补丁信息： http://www.monitorix.org/
CNVD-2013-14780	phpMyFAQ Ajax 文件和图像管理程序任意文件上传漏洞	高	暂无
CNVD-2013-14789	CiviCRM 存在多个 SQL 注入漏洞	高	CiviCRM 4.2.12, 4.3.7, 4.4 beta4 已经修复该漏洞，建议用户下载更新： http://www.civicrm.org
CNVD-2013-14792	UMPlayer 不安全库加载漏洞	高	暂无
CNVD-2013-14793	Google Caja JavaScript 解析器任意远程代码执行漏洞	高	厂商已经发布了升级补丁以修复这个漏洞： https://code.google.com/p/google-caj

			a/source/browse/trunk/src/com/google/caja/parser/js/Parser.java
CNVD-2013-14763	Gummy Bear Studios FTP Drive + HTTP Server 目录遍历漏洞	高	暂无
CNVD-2013-14765	Interstage Application Server/Studio 日志功能缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： http://www.fujitsu.com/global/support/software/security/products-f/interstage-201302e.html
CNVD-2013-14737	Light Alloy '.m3u'文件缓冲区溢出漏洞	高	暂无
CNVD-2013-14706	D-Link DES-3800 系列 WEB 管理实现远程拒绝服务漏洞	高	D-Link Japan DES-3800 firmware R4.50B58 已经修复该漏洞，建议用户下载更新： http://www.dlink-jp.com/
CNVD-2013-14719	Rackspace Windows Agent and Updater 未签名代理更新远程代码执行漏洞	高	Rackspace Windows Agent and Updater 1.2.6.1 不受该漏洞影响，用户可下载更新以修复该漏洞： http://www.rackspace.com/

表 3 部分高危漏洞列表

小结：本周，Apache、IBM、Cisco、ABB 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，使程序崩溃，导致拒绝服务攻击。相关漏洞影响工控行业，用户需尽快下载补丁更新，避免引发漏洞相关的网络安全事件。此外，Thomson Reuters Velocity Analytics 软件被披露存在一个高危零日漏洞，建议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、Xen 修补 2 个漏洞

Xen 是一款开放源代码的虚拟机。Xen 修补两个漏洞：Xen page_alloc_lock 和 mm_rwlock 锁逆序漏洞；Xen 'hvm_do_hypercentr()'本地权限提升漏洞。避免攻击者触发死锁使整个宿主系统崩溃或提升本地权限。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/patchInfo/show/41346>

<http://www.cnvd.org.cn/patchInfo/show/41347>



本周要闻速递

1. 谷歌 Nexus 设备存短信漏洞

荷兰某科技公司的 IT 管理员波格丹·阿里库(Bogdan Alecu)日前发现谷歌的 Galaxy Nexus、Nexus 4 和 Nexus 5 等智能手机存在短信漏洞,该漏洞易造成手机重启。据介绍,如果向谷歌 Nexus 智能手机发送大量的 0 级短信(Class 0 SMS),将会导致手机关闭网络服务或重启,不过他也表示目前还没有对所有的 Nexus 设备进行测试。尽管目前还不知道有多少 Android 设备会出现这一问题,但谷歌方面已经表示正在对该漏洞进行排查,并会即时发布补丁来修复该漏洞。此外,谷歌的 Play 应用商店中目前有一款名叫 Class0Firewall 的应用能够暂时阻止针对这一漏洞的恶意攻击。

参考链接: <http://mobile.163.com/13/1202/07/9F2RP1G80011179O.html>

2. Windows XP 用户面临新的 0day 漏洞攻击

一个新的 Windows 内核 0day 漏洞正被用于攻击 Windows XP 用户。微软已经证实了该漏洞,并发出了安全警告。该本地提权漏洞是与一个 Adobe Reader 漏洞结合起来入侵 Windows XP 机器,存在漏洞的 Adobe Reader 版本包括 9.5.4、10.1.6 和 11.0.02。该提权漏洞允许攻击者在内核模式下执行任意代码,包括安装恶意程序、浏览、修改或删除数据,创建拥有完整管理权限的帐号。安全公司建议 Windows XP 用户将 Adobe Reader 升级到最新版本,以及升级到较新的操作系统。

参考链接: <http://digi.163.com/13/1130/21/9EV8K87200162OUT.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是国家计算机网络应急技术处理协调中心的简称(英文简称为 CNCERT 或 CNCERT/CC),成立于 1999 年 9 月,是一个非政府非盈利的网络安全技术协调组织,主要任务是:按照“积极预防、及时发现、快速响应、力保恢复”的方针,开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作,以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前,CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时,CNCERT 积极开展国际合作,是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员,也是 APCERT 的发起人之一,致力于

构建跨境网络安全事件的快速响应和协调处置机制。截止 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 国际合作伙伴”关系。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999