

信息安全漏洞周报

2013 年 10 月 14 日-2013 年 10 月 20 日

2013 年第 42 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 131 个，其中高危漏洞 49 个、中危漏洞 75 个、低危漏洞 7 个。上述漏洞中，可利用来实施远程攻击的漏洞有 116 个。本周收录的漏洞中，已有 99 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“WebTester SQL 注入漏洞”、“InduSoft Thin Client 'novapi7.dll' ActiveX 控件缓冲区溢出漏洞”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 6 家成员单位及个人报送了本周收录的全部 131 个漏洞。各单位报送情况如表 1 所示。其中，安天实验室、天融信、启明星辰、绿盟科技等单位报送数量较多。此外，个人报送者向 CNVD 提交了 17 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	205	0
天融信	190	0
启明星辰	54	0
绿盟科技	52	0
恒安嘉新	39	0
东软	6	0
个人	17	17
报送总计	563	17

录入总计	131（去重）	17
------	---------	----

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、Cisco、HP 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	23	18%
2	Cisco	18	15%
3	HP	8	6%
	wordpress	7	5%
4	XenSource	5	4%
5	WebTester	4	3%
6	IBM	3	2%
7	FFmpeg	3	2%
8	Google	3	2%
10	Linux	1	1%
11	其它	56	42%

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 131 个漏洞。其中应用程序漏洞 73 个，WEB 应用漏洞 24 个，操作系统漏洞 6 个，网络设备漏洞 12 个，数据库漏洞 5 个，安全产品漏洞 11 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	73
WEB 应用漏洞	24
网络设备漏洞	12
操作系统漏洞	6
安全产品漏洞	11
数据库漏洞	5

表 3 漏洞按影响类型统计表

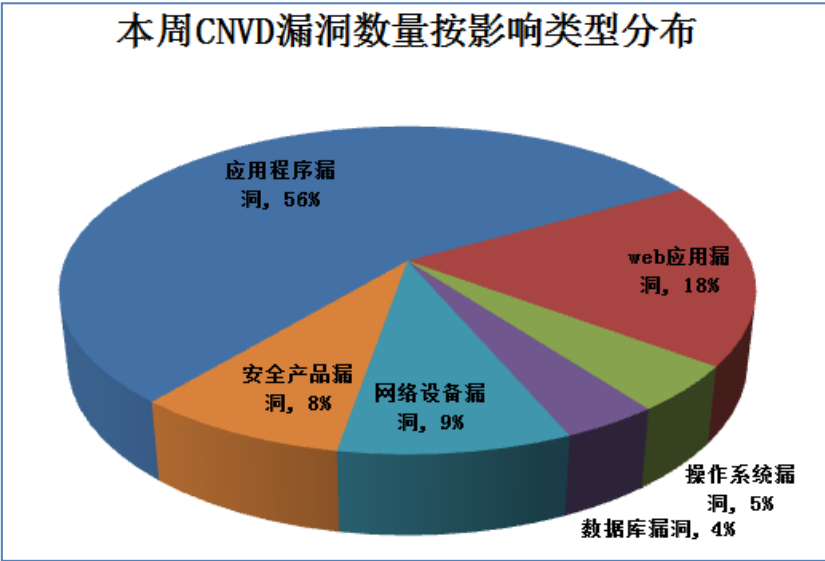


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 9 个电信行业漏洞、2 个移动互联网行业漏洞和 2 个工控系统行业漏洞（如下列表所示）。其中，“D-Link 路由器固件后门漏洞、BlackBerry Enterprise Service 远程代码执行漏洞、InduSoft Thin Client 'novapi7.dll' ActiveX 控件缓冲区溢出漏洞、Alstom e-Terracontrol DNP3 Master 存在未明输入处理远程拒绝服务漏洞”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-2013-13778	IBM WebSphere eXtreme Scale 监视控制台存在未明漏洞	中	是
电信	CNVD-2013-13762	Oracle MySQL Server 远程漏洞	低	是
电信	CNVD-2013-13773	Oracle Database Server 'XML Parser'组件远程漏洞	中	是
电信	CNVD-2013-13774	Oracle Database Server 'Core RDBMS'组件远程漏洞	中	是
电信	CNVD-2013-13777	D-Link 路由器固件后门漏洞	高	否
电信	CNVD-2013-13750	Agilent E5810A LAN/GPIB Gateway 存在多个漏洞	中	否
电信	CNVD-2013-13704	Cisco Unified IP Phones 9900 Series 固件升级命令注入漏洞	中	是
电信	CNVD-2013-13703	Cisco Unified IP Phones 9900 Series webapp 远程缓冲区溢出漏洞	中	是
电信	CNVD-2013-13671	ONO Hitron CDE-30364	中	否

		Router 远程拒绝服务漏洞		
移动互联网	CNVD-2013-13700	WhatsApp 信息泄露漏洞	中	否
移动互联网	CNVD-2013-13687	BlackBerry Enterprise Service 远程代码执行漏洞	高	是
工控系统	CNVD-2013-13776	InduSoft Thin Client 'novapi7.dll' ActiveX 控件缓冲区溢出漏洞	高	否
工控系统	CNVD-2013-13689	Alstom e-Terracontrol DNP3 Master 存在未明输入处理远程拒绝服务漏洞	高	是

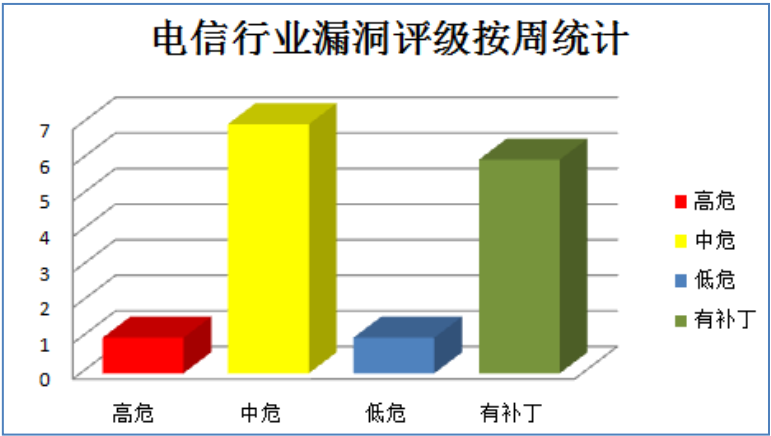


图 1 电信行业漏洞统计

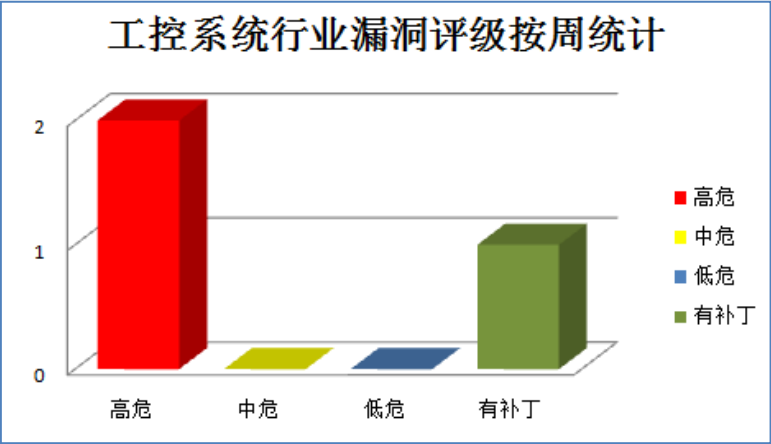


图 2 工控系统行业漏洞统计

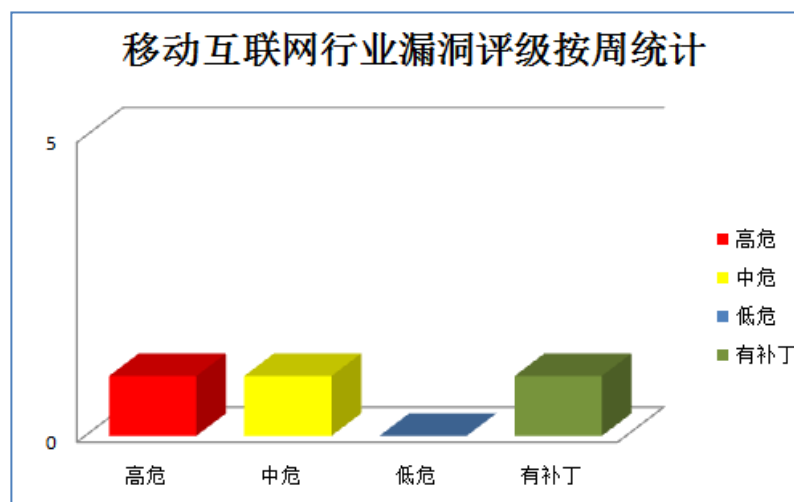


图 3 移动互联网行业漏洞统计

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、Oracle 产品安全漏洞

Oracle MySQL Server 是一款关系型数据库系统；Oracle Java Runtime Environment 是一款为 JAVA 应用程序提供可靠运行环境的解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Oracle Java SE 远程漏洞（CNVD-2013-13789、CNVD-2013-13791、CNVD-2013-13792、CNVD-2013-13793、CNVD-2013-13761、CNVD-2013-13764、CNVD-2013-13766）、Oracle MySQL Server 远程漏洞（CNVD-2013-13798）等。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-2013-13789>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13791>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13792>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13793>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13798>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13761>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13764>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13766>

2、Cisco 产品安全漏洞

Cisco Firewall Services Module 是一款防火墙服务模块；Cisco Adaptive Security

Appliance 是一款自适应安全设备，可提供安全和 VPN 服务的模块。本周，上述思科产品被披露存在多个安全漏洞，攻击者利用漏洞可使设备重载，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco 多个产品 SQL*Net 检测引擎畸形 TNS 报文处理远程拒绝服务漏洞、Cisco Adaptive Security Appliance Clientless SSL VPN 特制 HTTPS 请求远程拒绝服务漏洞、Cisco Adaptive Security Appliance DNS 检测拒绝服务漏洞、Cisco Adaptive Security Appliance HTTP DPI 畸形应答处理远程拒绝服务漏洞、Cisco Adaptive Security Appliance ASDM 特制证书验证绕过漏洞、Cisco Adaptive Security Appliance 特制证书验证绕过漏洞、Cisco Adaptive Security Appliance IPsec VPN 特制 ICMP 报文处理远程拒绝服务漏洞、Cisco Adaptive Security Appliance AnyConnect SSL VPN 远程拒绝服务漏洞等。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-2013-13677>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13679>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13680>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13681>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13682>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13684>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13685>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13686>

3、HP 产品安全漏洞

HP Business Process Monitor 是一款业务流程和性能监控解决方案；惠普智能管理中心(HP IMC)是一款独立的综合管理平台，提供新一代集成的模块化网络管理功能。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，执行任意代码。

CNVD 收录的相关漏洞包括：HP Business Process Monitor 存在未明远程代码执行漏洞、HP 多个产品存在未明信息泄露漏洞、HP 多个产品存在未明远程代码执行漏洞、HP 多个产品存在未明 SQL 注入漏洞、HP 多个产品存在未明远程信息泄露漏洞、HP IMC Service Operation Management Software 验证绕过漏洞、HP Business Process Monitor 远程代码执行漏洞、HP 多个产品存在未明未授权访问漏洞。其中，除“HP Business Process Monitor 远程代码执行漏洞、HP 多个产品存在未明未授权访问漏洞”外，其余的综合评级均为“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-2013-13742>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13672>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13673>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13674>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13695>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13676>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13729>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13675>

4、Google Chrome 安全漏洞

Google Chrome 是一款 WEB 浏览器。本周，该产品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，执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 内存错误引用远程代码执行漏洞（CNVD-2013-13790、CNVD-2013-13755）、Google Chrome 存在多个未明漏洞（CNVD-2013-13756）。其中，“Google Chrome 内存错误引用远程代码执行漏洞（CNVD-2013-13790、CNVD-2013-13755）”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/flaw/show/CNVD-2013-13790>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13755>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13756>

5、WebTester SQL 注入漏洞

WebTester 是一款在线测试和测试生成、管理、分析的解决方案。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 startTest.php 页面未能充分过滤 TestID 参数，攻击者利用漏洞可操作和获取数据库的敏感数据。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-2013-13751>

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-2013-13780	Drupal Context 模块任意 PHP 代码执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://drupal.org/
CNVD-2013-13758	Dolibarr 'sondage'参数 SQL 注入漏洞	高	用户可联系供应商获得补丁信息： http://www.dolibarr.org/
CNVD-2013-13771	BilboPlanet 'auth.php' SQL 注入漏洞	高	暂无
CNVD-2013-13776	InduSoft Thin Client 'novapi7.dll' ActiveX 控件缓冲区溢出漏洞	高	暂无

CNVD-2013-13739	Imperva SecureSphere Web Application Firewall 搜索字段 SQL 注入漏洞	高	Imperva SecureSphere Web Application Firewall MX 9.5.6 Patch 8.0 (August 30, 2013)已经修改该漏洞，建议用户下载更新： http://www.imperva.com
CNVD-2013-13712	SolarWinds Server & Application Monitor Pepco32c.ocx 'PEstrarg1' 缓冲区溢出漏洞	高	暂无
CNVD-2013-13754	WebTester 任意文件上传漏洞	高	暂无
CNVD-2013-13699	WordPress 插件 Landing Pages 'post'参数 SQL 注入漏洞	高	WordPress Landing Pages Plugin 1.2.3 (10/09/13)已经 http://wordpress.org/plugins/landing-pages
CNVD-2013-13738	Internet Haut Debit Mobile NetConfig.ini 文件处理缓冲区溢出漏洞	高	暂无
CNVD-2013-13696	Xen libxl_list_cpupool 多线程 Toolstack 内存错误引用拒绝服务漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： http://seclists.org/oss-sec/2013/q4/att-60/xsa70.patch

表 3 部分高危漏洞列表

小结：本周，Oracle、Cisco、HP 多款产品以及 Google Chrome 被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息，导致拒绝服务攻击或执行任意代码。此外，WebTester 程序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、Linux kernel scm_check_creds 权限提升漏洞

Linux Kernel 是 Linux 操作系统的内核。本周，Linux 发布安全公告，修补 Linux kernel 3.11 之前版本存在的漏洞。攻击者可以利用漏洞提升权限。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/patchInfo/show/40201>

本周要闻速递

1. 微软修复 SetMouseCapture IE 零日漏洞

微软 2013 年 10 月份的安全更新发布了 8 个公告，修复了 26 个漏洞，其中最具影响力的补丁是解决了最近 IE 浏览器出现的零日漏洞。根据零日漏洞 CVE-2013-3893 的调查结果，微软表示，该漏洞是由于 IE“访问了内存中已被删除或没有正确分配的对象”产生的。这样，攻击者就可以执行任意代码，华盛顿 Redmond 总部软件专家表示，攻击者可以建立一个特定的网站，利用该漏洞来欺骗用户访问它。

参考链接：<http://sec.chinabyte.com/13/12746013.shtml>

2. 甲骨文修补安全漏洞

本周二，甲骨文公司修复了 Java、数据库及其它产品当中存在的 127 项安全问题，同时修复了某些可能允许攻击者接管系统的严重漏洞。在此次 Java 安全更新中被修复的 51 项漏洞当中，有 40 项只影响客户端部署，其中包括经常成为攻击目标的 Java 网络浏览器插件以及 8 项既影响客户端又影响服务器部署的漏洞。恶意人士可以通过 Java Web Start 应用或者 Java 程序利用这些漏洞。甲骨文将在本月推出的重要补丁更新咨文中详尽列举每款产品中得以修复的具体漏洞数量、严重程度评分以及漏洞所影响的具体产品版本。

参考链接：<http://sec.chinabyte.com/34/12750534.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