

信息安全漏洞周报

2014 年 5 月 5 日-2014 年 5 月 11 日

2014 年第 19 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 180 个，其中高危漏洞 67 个、中危漏洞 96 个、低危漏洞 17 个。上述漏洞中，可利用来实施远程攻击的漏洞有 158 个。本周收录的漏洞中，已有 145 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“Caldera 存在多个 SQL 注入漏洞”、“NULL NUKE CMS 'admin.php'存在多个漏洞”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、合作伙伴及个人报送了本周收录的全部 180 个漏洞。报送情况如表 1 所示。其中，安天实验室、天融信、启明星辰等单位报送数量较多。此外，CNCERT 各分中心、习科网络安全、High-Tech Bridge Security Research Lab、汉柏科技有限公司及多个白帽子向 CNVD 提交了 51 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	144	0
天融信	98	0
启明星辰	62	0
恒安嘉新	48	0
习科网络安全	24	24
CNCERT 山西分中心	9	9
CNCERT 黑龙江分中心	2	2

CNCERT 青海分中心	1	1
CNCER 新疆分中心	1	1
汉柏科技有限公司	1	1
High-Tech Bridge Security Research Lab	2	2
个人	11	11
报送总计	403	51
录入总计	180（去重）	51

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cisco、IBM、Mozilla 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	Cisco	30	17%
2	IBM	15	8%
3	Mozilla	13	7%
4	SAP	7	4%
5	Apache	5	3%
6	WordPress	5	3%
7	Linux	3	2%
8	Drupal	3	2%
9	Google	2	1%
10	其他	97	53%

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 180 个漏洞。其中应用程序漏洞 118 个，WEB 应用漏洞 41 个，操作系统漏洞 11 个，网络设备漏洞 6 个，安全产品漏洞 4 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	118
WEB 应用漏洞	41
操作系统漏洞	11
网络设备漏洞	6
安全产品漏洞	4

表 3 漏洞按影响类型统计表

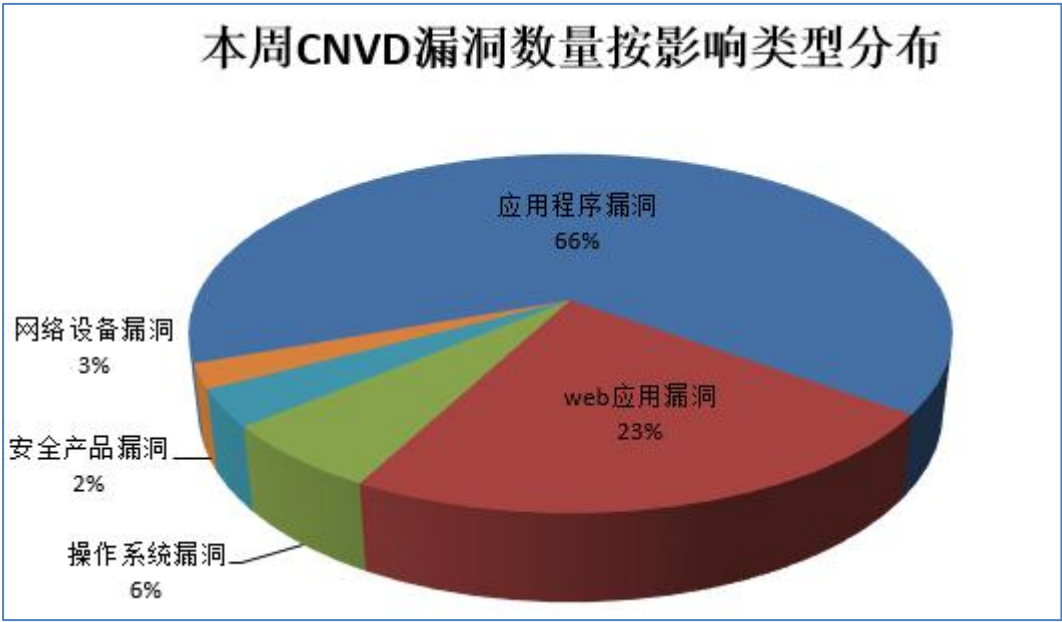


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 12 个电信行业漏洞、2 个移动互联网行业漏洞、3 个工控系统行业漏洞（如下列表所示）。其中，“Amtelco miSecureMessages 会话管理信息泄露漏洞”的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2014-02819	Cisco WebEx Meetings Server 跨站请求伪造漏洞	中	否
电信	CNVD-2014-02822	Beetel 450TC2 Router 跨站请求伪造漏洞	中	否
电信	CNVD-2014-02835	IBM WebSphere Application Server 信息泄露漏洞（CNVD-2014-02835）	中	是
电信	CNVD-2014-02834	IBM WebSphere Application Server 信息泄露漏洞（CNVD-2014-02834）	中	是
电信	CNVD-2014-02839	IBM Tivoli Netcool/OMNIBus 跨站脚本漏洞	低	是
电信	CNVD-2014-02838	IBM Tivoli Netcool/OMNIBus WebGUI 跨站脚本漏洞	低	是
电信	CNVD-2014-02837	IBM WebSphere Application Server Liberty Profile 信息泄	中	是

		露漏洞（CNVD-2014-02837）		
电信	CNVD-2014-02836	IBM WebSphere Application Server 远程拒绝服务漏洞（CNVD-2014-02836）	中	是
电信	CNVD-2014-02891	NETGEAR DGN2200 ADSL 路由器跨站请求伪造漏洞	低	否
电信	CNVD-2014-02911	Cisco Nexus 1000V IGMPv2/IGMPv3 访问控制缺陷安全绕过漏洞	中	是
电信	CNVD-2014-02932	Cisco NX-OS 本地拒绝服务漏洞	中	是
电信	CNVD-2014-02924	IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2014-02924）	低	是
移动互联网	CNVD-2014-02783	Amtelco miSecureMessages 会话管理信息泄露漏洞	高	是
移动互联网	CNVD-2014-02914	Apple iOS email 附件不加密本地信息泄露漏洞	低	否
工控系统	CNVD-2014-02840	ABB UNITROL 1000 Series Commissioning and Maintenance Tool 任意文件覆盖漏洞	中	是
工控系统	CNVD-2014-02852	ABB AC800M MMS(Manufacture Message Standard) Initiate Request 报文缓冲区溢出漏洞	高	否
工控系统	CNVD-2014-02853	ABB AC800M MMS(Manufacture Message Standard) Initiate Request 报文异常取值拒绝服务漏洞	高	否

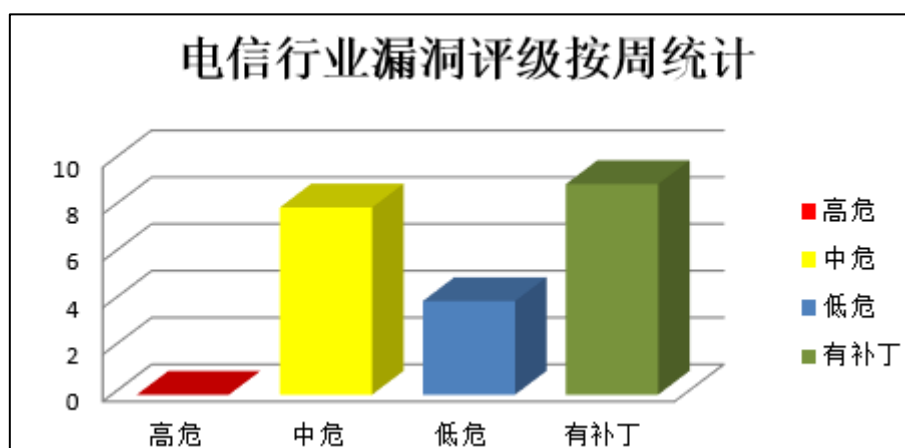


图 1 电信行业漏洞统计

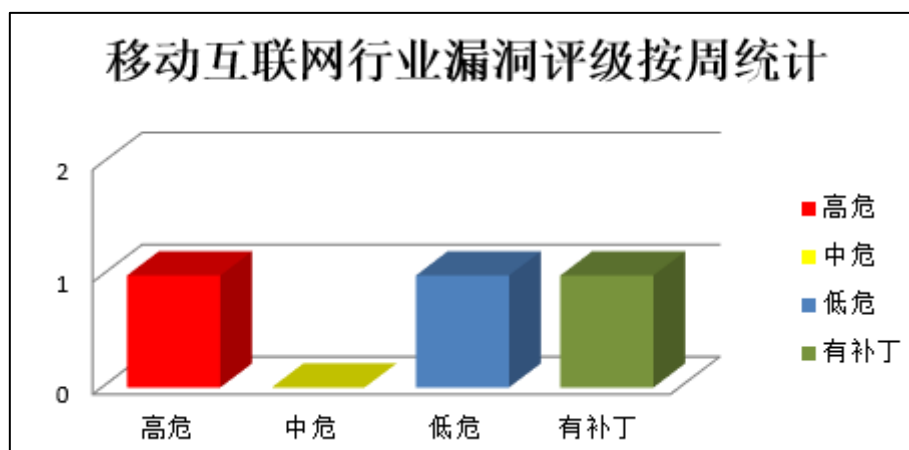


图 2 移动互联网行业漏洞统计

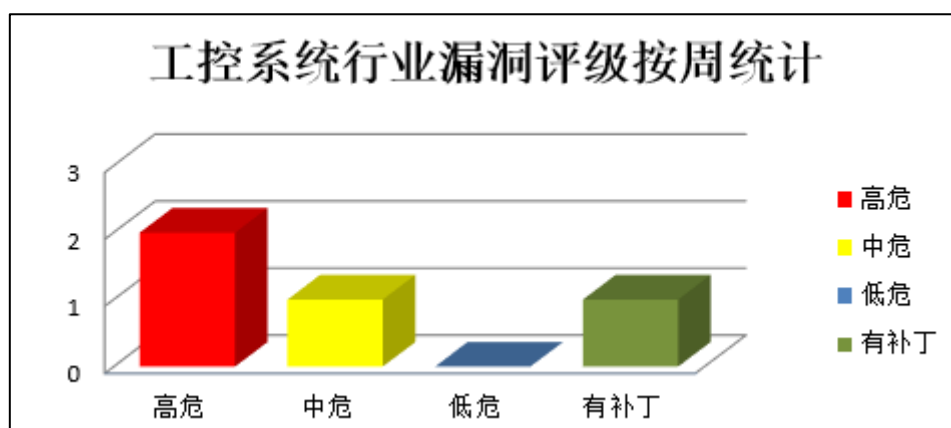


图 3 工控行业漏洞统计

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、OAuth 产品安全漏洞

OAuth(开放授权)是一个开放标准，允许第三方网站在用户授权的前提下访问在用户在服务商那里存储的各种信息，而这种授权无需将用户提供用户名和密码提供给该第三方网站。本周，上述产品被披露存在开放重定向和信息泄露漏洞，攻击者可利用漏洞构建恶意 URI，诱使用户解析，进行开放重定向攻击或通过引诱用户登录钓鱼网站，从而读取其在网站上存储的敏感信息。该漏洞的综合评级为“高危”。目前，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-2014-02785>

2、Cisco 产品安全漏洞

Cisco WebEx 是 Cisco 公司提供的网络会议解决方案。Cisco WebEx Player 用于播放与会者在电脑上所记录的 WebEx 会议记录。Cisco TelePresence 是思科公司开发的网

真会议解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco WebEx ARF Player .arf 文件解析内存破坏漏洞（CNVD-2014-02902）、Cisco WebEx WRF 和 ARF Player 越界读拒绝服务漏洞、Cisco TelePresence TC 和 TE 软件 SIP 拒绝服务漏洞（CNVD-2014-02826、CNVD-2014-02827、CNVD-2014-02828）。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-2014-02902>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02903>

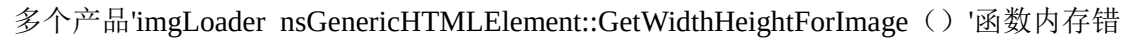
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02826>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02827>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02828>

3、Mozilla 产品安全漏洞

Mozilla Firefox/Thunderbird/SeaMonkey 是 Mozilla 所发布的 WEB 浏览器和邮件/新闻组客户端。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞在受影响用户应用程序的上下文中执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Mozilla Firefox/SeaMonkey 越界内存破坏漏洞、Mozilla Firefox/Thunderbird/SeaMonkey 内存错误引用漏洞（CNVD-2014-02816）、Mozilla 多个产品函数内存错误引用漏洞、Mozilla 多个产品 Web Notification API 特制源组件任意代码执行漏洞、Mozilla 多个产品函数内存错误引用漏洞。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网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02851>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02816>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02794>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02793>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02790>

4、Apache 产品安全漏洞

Apache Struts 框架是一个基于 Java Servlets,JavaBeans, 和 JavaServer Pages (JSP) 的 Web 应用框架的开源项目。Apache CXF 是一个开源服务框架，用于使用 JAX-WS、JAX-RS 等前端编程 API 编译和开发服务。本周，上述产品被披露存在安全绕过和拒绝服务漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apache Struts ClassLoader 操作安全绕过漏洞（CNVD-2014-02775）、Apache Struts 'CookieInterceptor'安全绕过漏洞、Apache CXF 远程拒绝服

务漏洞（CNVD-2014-02895）。其中，“Apache Struts ClassLoader 操作安全绕过漏洞（CNVD-2014-02775）”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/flaw/show/CNVD-2014-02775>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02855>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02775>

5、Typo3 si_bibtex Extension 存在多个漏洞

Typo3 是开源内容管理系统。本周，Typo3 被披露存在综合评级为“高危”的 SQL 注入和 HTML 注入漏洞。由于 Typo3 si_bibtex Extension 未能正确过滤用户通过"search"和"list"提交的输入，允许远程攻击者利用漏洞提交特制的 SQL 查询，操作或获取数据库数据。目前，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-2014-02762>

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-2014-02754	PaperCut MF 存在未明漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.papercut-mf.com/release-history/
CNVD-2014-02764	AlienVault OSSIM 存在多个 SQL 注入漏洞	高	AlienVault OSSIM 4.3.2 已经修复该漏洞，建议用户下载更新： http://www.alienvault.com/
CNVD-2014-02771	Debian Linux Super 'setuid()'函数 RLIMIT_NPROC 处理特权提升漏洞	高	Debian 3.30.0-3+squeeze2, 3.30.0-6+deb7u1 已经修复该漏洞，建议用户下载更新： http://www.debian.org/
CNVD-2014-02767	WordPress File Gallery 插件远程 PHP 代码执行漏洞	高	WordPress File Gallery 1.7.9.2 已经修复该漏洞，建议用户下载更新： http://wordpress.org/plugins/file-gallery/
CNVD-2014-02782	Python virtualenvwrapper 模块不安全文件权限漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： https://bitbucket.org/dhellmann/virtualenvwrapper/commits/04f897165c1eb84e6fe52442b0a8fc9f01915aa6
CNVD-2014-02784	RXVT-Unicode 远程命令执行漏洞	高	rxvt-unicode-9.20 已经修复该漏洞，建议用户下载更新： http://dist.schmorp.de/rxvt-unicode/C

			hanges
CNVD-2014-02783	Amtelco miSecureMessages 会话管理信息泄露漏洞	高	miSecureMessages 6.3 已经修复该漏洞，建议用户下载更新： https://www.amtelco.com
CNVD-2014-02804	Citrix NetScaler 存在未明漏洞	高	Citrix NetScaler Application Delivery Controller (ADC)和 NetScaler Gateway 9.3-66.5 或 10.1-122.17 已经修复该漏洞，建议用户下载更新： http://support.citrix.com/article/CTX140651
CNVD-2014-02806	Citrix NetScaler 证书校验安全绕过漏洞	高	Citrix NetScaler Application Delivery Controller (ADC)和 NetScaler Gateway 9.3-66.5 或 10.1-122.17 已经修复该漏洞，建议用户下载更新： http://support.citrix.com/article/CTX140651
CNVD-2014-02807	dpkg 目录遍历漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.debian.org/security/2014/dsa-2915

表 3 部分高危漏洞列表

小结：本周，OAuth 被披露存在开放重定向和信息泄露漏洞，攻击者可利用漏洞构建恶意 URI，诱使用户解析，进行开放重定向攻击或通过引诱用户登录钓鱼网站，从而读取其在网站上存储的敏感信息。此外，Cisco、Mozilla、Apache 集中披露多款产品存在多个漏洞，攻击者可利用漏洞获取敏感信息、执行任意代码或发起拒绝服务攻击。另外，Typo3 被披露存在一个高危零日漏洞，攻击者可利用漏洞提交特制的 SQL 查询，操作或获取数据库数据。CNVD 已经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、IBM 修补 Security Access Manager for Web 产品漏洞

IBM Security Access Manager 软件是高度可扩展的用户认证、授权和 Web SSO 解决方案,用于在各种 Web 和应用资源上实施安全策略,集中管理在线门户网站。

本周，IBM 修补了上述产品存在的远程拒绝服务漏洞，避免远程攻击者利用漏洞提交特殊请求，可消耗大量 CPU 利用率，使应用程序崩溃，造成拒绝服务攻击。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网络安全事件。

补丁下载链接: <http://www.cnvd.org.cn/patchInfo/show/45465>



本周要闻速递

1. ios 7 最新安全漏洞: 所有邮件附件未加密

北京时间 5 月 5 日晚间消息, 德国 NESO 安全实验室专家安德利亚斯·库尔茨(Andreas Kurtz)近日在 iOS 7 中发现一处安全漏洞, 即 iOS 7 设备所发送的电子邮件附件均为未加密状态。库尔茨用一台升级到 iOS 7.1 的 iPhone 4 证实了这一漏洞。升级后, 库尔茨设置了一个 IMAP 邮箱帐号, 并测试了带有附件的邮件。关机后访问文件系统时, 他发现文件是用明文显示的。库尔茨称, 该漏洞至少影响 iOS 7.0.4 至最新的 7.1.1 版本。库尔茨还称, 他之前已经将该漏洞报告给苹果公司。苹果的公司的答复是, 已经了解该问题, 但何时修改该漏洞还没有明确时间表。

参考链接: <http://tech.sina.com.cn/it/2014-05-05/22159359679.shtml>

2. iOS 7.1.1 又现锁屏漏洞

之前, 苹果从 iOS 6 开始就不断爆出与锁屏有关的漏洞, 经过一次又一次的修复, 最终苹果发布了 iOS 7.1 版本, 并声称解决了绝大多数 BUG 和漏洞, 不过绝大多数并不意味着所有。最近有人爆料, iOS 7.1.1 存在着相当严重的安全漏洞, 可以越过锁屏界面查看联系人等。

参考链接: <http://www.techweb.com.cn/ucweb/news/id/2033994>

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

国家计算机网络应急技术处理协调中心 (简称“国家互联网应急中心”, 英文简称是 CNCERT 或 CNCERT/CC), 成立于 2002 年 9 月, 为非政府非盈利的网络安全技术中心, 是我国网络安全应急体系的核心协调机构。

作为国家级应急中心, CNCERT 的主要职责是: 按照“积极预防、及时发现、快速响应、力保恢复”的方针, 开展互联网网络安全事件的预防、发现、预警和协调处置等工作, 维护国家公共互联网安全, 保障基础信息网络和重要信息系统的安全运行。

网址: www.cert.org.cn

邮箱: vreport@cert.org.cn

电话: 010-82990999