

信息安全漏洞周报

2014 年 4 月 28 日-2014 年 5 月 4 日

2014 年第 18 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 105 个，其中高危漏洞 54 个、中危漏洞 48 个、低危漏洞 3 个。上述漏洞中，可利用来实施远程攻击的漏洞有 95 个。本周收录的漏洞中，已有 68 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“IE6-IE11 V GX.DLL 远程代码执行漏洞”、“Unitrends Enterprise Backup 'comm'命令执行漏洞”、“GeoCore 存在多个 SQL 注入漏洞”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、合作伙伴及个人报送了本周收录的全部 105 个漏洞。报送情况如表 1 所示。其中，启明星辰、天融信、安天实验室等单位报送数量较多。此外，CNCERT 各分中心、国家互联网应急中心、习科网络安全及多个白帽子向 CNVD 提交了 71 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	145	0
天融信	98	0
安天实验室	53	0
恒安嘉新	10	0
绿盟科技	1	0
知道创宇	1	0
习科网络安全	18	18

国家互联网应急中心	2	2
CNCERT 江西分中心	21	21
CNCERT 安徽分中心	12	12
CNCERT 山东分中心	7	7
CNCERT 黑龙江分中心	3	3
CNCERT 山西分中心	2	2
CNCERT 新疆分中心	1	1
个人	5	5
报送总计	379	71
录入总计	105（去重）	71

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、WordPress、Google 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	12	11%
2	WordPress	8	8%
3	Google	7	7%
4	Microsoft	6	6%
5	Drupal	6	6%
6	Apache	4	4%
7	Simple	3	3%
8	Siemens	2	2%
9	IBM	1	1%
10	其它	56	52%

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 105 个漏洞。其中应用程序漏洞 68 个，WEB 应用漏洞 22 个，网络设备漏洞 10 个，操作系统漏洞 3 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	68
WEB 应用漏洞	22

网络设备漏洞	10
操作系统漏洞	3
安全产品漏洞	2

表 3 漏洞按影响类型统计表

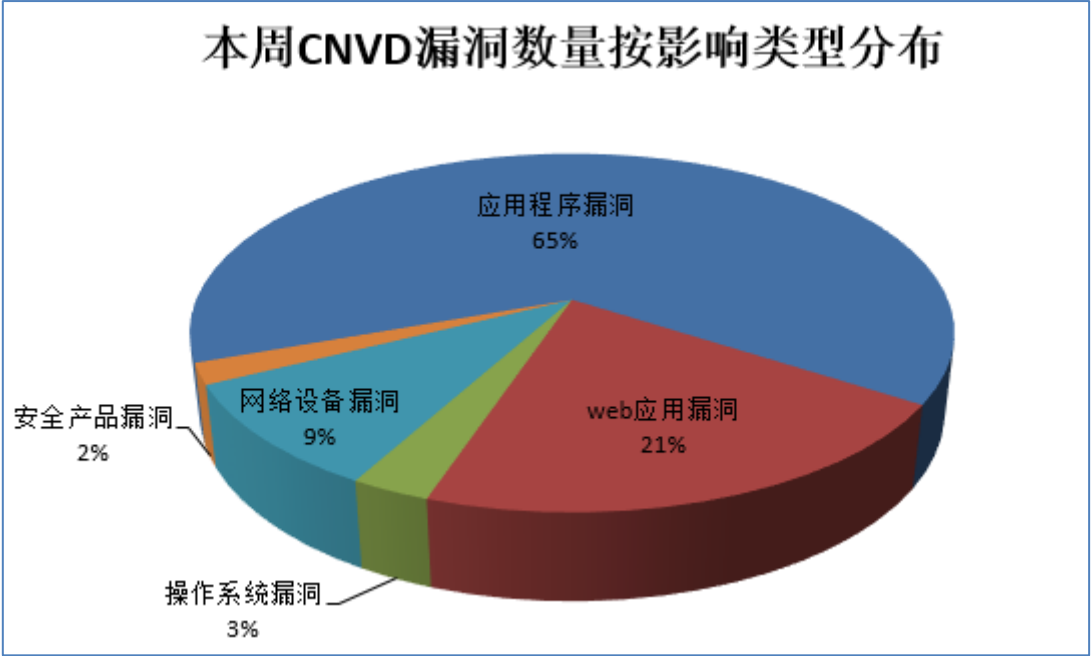


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 11 个电信行业漏洞、3 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，“Google Android 信息泄露漏洞、InduSoft Web Studio NTWebServer 目录遍历漏洞”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-2014-02652	Cisco IOS 拒绝服务漏洞（CNVD-2014-02652）	中	是
电信	CNVD-2014-02653	Cisco IOS 拒绝服务漏洞（CNVD-2014-02653）	中	是
电信	CNVD-2014-02672	Cisco IOS ACL 拒绝服务漏洞	中	是
电信	CNVD-2014-02673	Cisco IOS BGP 路由器进程拒绝服务漏洞	中	是
电信	CNVD-2014-02674	Cisco IOS 拒绝服务漏洞（CNVD-2014-02674）	中	是
电信	CNVD-2014-02675	Cisco IOS 拒绝服务漏洞（CNVD-2014-02675）	中	是

电信	CNVD-2014-02698	Comtrend CT-5361T 路由器 dd nsmngr.cmd username 参数跨站脚本漏洞	中	否
电信	CNVD-2014-02720	Cisco Unified Communications Manager 信息泄露漏洞 (CNVD-2014-02720)	中	是
电信	CNVD-2014-02719	Cisco Unified Communications Manager 信息泄露漏洞 (CNVD-2014-02719)	中	是
电信	CNVD-2014-02729	NETGEAR DGN1000 未文档化 scfgmgr 服务漏洞	高	否
电信	CNVD-2014-02737	Cisco IOS XE Software L2TP 报文处理拒绝服务漏洞	中	是
移动互联网	CNVD-2014-02745	Birebin.com application for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-02744	Misli.com application for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-02752	Google Android 信息泄露漏洞	高	是
工控系统	CNVD-2014-02659	Siemens SIMATIC S7-1200 跨站脚本漏洞	中	是
工控系统	CNVD-2014-02657	Siemens SIMATIC S7-1200 HTTP 头注入漏洞	中	是
工控系统	CNVD-2014-02688	InduSoft Web Studio NTWeb Server 目录遍历漏洞	高	是

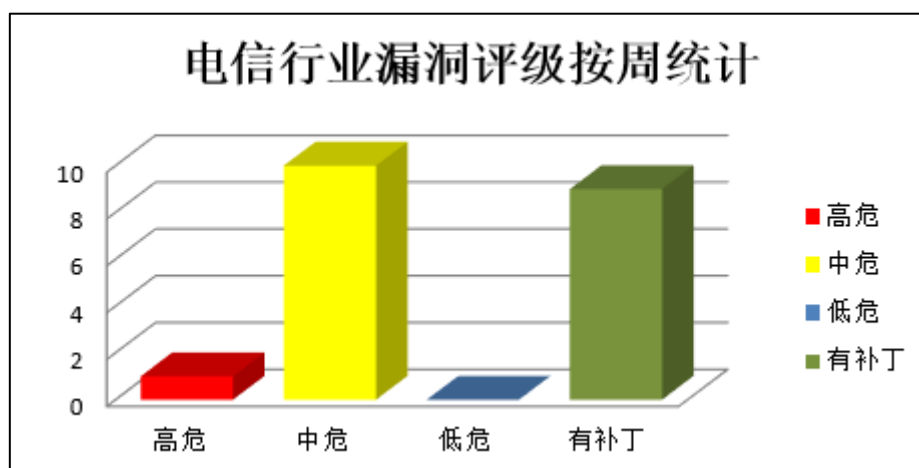


图 1 电信行业漏洞统计

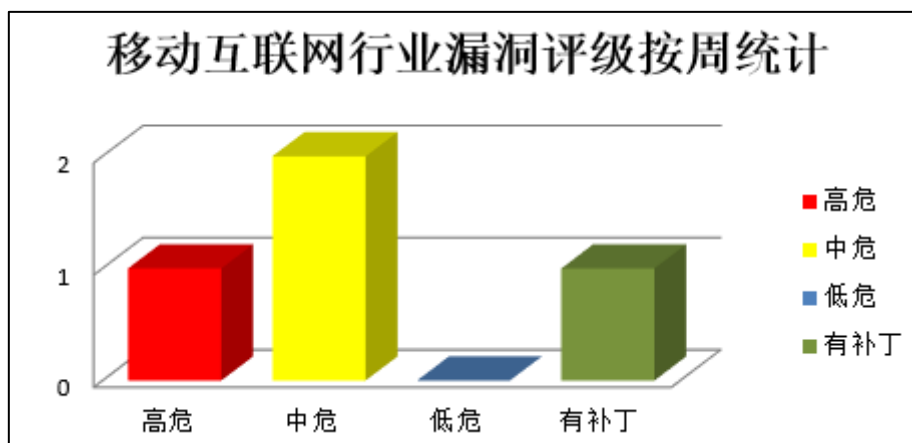


图 2 移动互联网行业漏洞统计

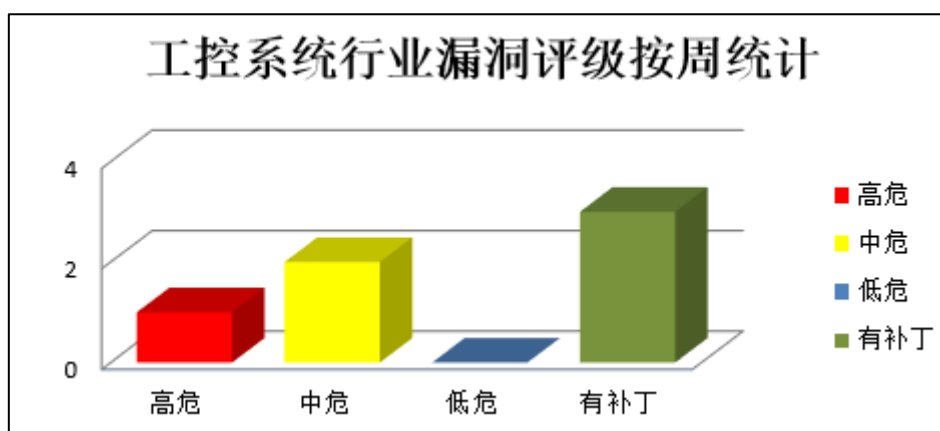


图 3 工控行业漏洞统计

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、Microsoft Internet Explorer 安全漏洞

Microsoft Internet Explorer 是一款 WEB 浏览器。本周，该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。

其中，影响较为严重的为：Microsoft Internet Explorer VGX.DLL 代码执行高危零日漏洞。漏洞存在于 IE6 至 IE11 等版本的 VGX.DLL 中，VGX.DLL 是 IE 中负责渲染 VML 的组件，该组件未对正确处理内存对象释放机制，可被利用发起基于内存释放后重用技术的攻击，且攻击代码可以绕过微软现有的 ASLR 和 DEP 安全机制。攻击者可以诱使用户访问特定构造的一个网站页面，在网站页面上放置恶意代码，从而发起大规模挂马攻击。漏洞详情可参考 CNVD 网站公告。

CNVD 收录的其他漏洞包括：Microsoft Internet Explorer 存在未明漏洞（CNVD-2014-02746）、Microsoft Internet Explorer 对象混淆漏洞（CNVD-2014-02704 、CNVD-20

14-02731)、Microsoft Internet Explorer 内存错误引用漏洞 (CNVD-2014-02703)。上述漏洞的综合评级均为“高危”。目前, 厂商尚未发布上述漏洞的修补程序, 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-2014-02648>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02746>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02704>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02731>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02703>

2、Apache 产品安全漏洞

Apache Struts 是一款开放源代码架构; Apache Struts2 是第二代企业级 web 应用框架。Apache Harmony 是 Apache 软件基金会的开源项目。本周, 上述产品被披露存在安全机制绕过漏洞, 攻击者可利用漏洞执行未授权操作。

CNVD 收录的相关漏洞包括: Apache Struts 'getClass()'方法安全绕过漏洞、Apache Struts2 S2-020 漏洞补丁存在被绕过漏洞、Apache Struts 类加载器安全绕过漏洞、Apache Harmony 安全机制绕过漏洞。其中, “Apache Struts 'getClass()'方法安全绕过漏洞、Apache Struts2 S2-020 漏洞补丁存在被绕过漏洞”的综合评级均为“高危”。除“Apache Struts2 S2-020 漏洞补丁存在被绕过漏洞”外, 厂商已经发布了其余漏洞的修补程序。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-2014-02705>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02661>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02702>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02751>

3、Cisco 产品安全漏洞

Cisco Unified Contact Center Express 是联系中心解决方案; 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; Cisco Unified Communications Manager 是呼叫处理组件; Cisco IOS 是多数思科系统路由器和网络交换机上使用的互联网络操作系统。本周, 上述产品被披露存在拒绝服务、文件上传和信息泄露漏洞, 攻击者可利用漏洞发起拒绝服务攻击、获取敏感信息和执行任意代码。

CNVD 收录的相关漏洞包括: Cisco Adaptive Security Appliance (ASA) 软件拒绝服务漏洞、Cisco Unified Contact Center Express 任意文件上传漏洞、Cisco Unified Communications Manager 信息泄露漏洞 (CNVD-2014-02719、CNVD-2014-02720)、Cisco IOS XE Software L2TP 报文处理拒绝服务漏洞。除“Cisco Unified Contact Center Express 任意文件上传漏洞”外, 厂商已经发布了其余漏洞的修补程序。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-2014-02717>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02718>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02719>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02720>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02737>

4、Google 产品安全漏洞

Google Chrome 是一款 WEB 浏览器。Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的开源操作系统。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息或拒绝服务。

CNVD 收录的相关漏洞包括：Google Android 信息泄露漏洞、Google Chrome V8 访问限制漏洞、Google Chrome 内存错误引用漏洞（CNVD-2014-02710）、Google Chrome Blink 输入验证漏洞、Google Chrome 输入验证漏洞（CNVD-2014-02711）。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-2014-02752>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02713>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02710>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02712>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02711>

5、Python Image Library 任意命令执行漏洞

Python Image Library 是读写图像文件的应用库。本周，Python 被披露存在一个综合评级为“高危”的任意命令执行漏洞。由于 Python Image Library 和 Pillow 处理用户提交的包含 shell 元字符数据的输入缺少充分过滤，允许远程攻击者利用漏洞执行任意代码。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-2014-02739>

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-2014-02660	Unitrends Enterprise Backup 'comm'命令执行漏洞	高	暂无
CNVD-2014-02662	iDevAffiliate 'idevads.php' SQL 注入漏洞	高	暂无

CNVD-2014-02651	Pimcore 'Pimcore_Tool_Newsletter::getObjectByToken()' PHP 对象注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.pimcore.org/en/resources/blog/pimcore+2.2+released_b442
CNVD-2014-02682	LifeSize UVC '/server-admin/operations/diagnose/trace/'远程代码执行漏洞	高	暂无
CNVD-2014-02681	LifeSize UVC '/server-admin/operations/diagnose/dns/'远程代码执行漏洞	高	暂无
CNVD-2014-02680	LifeSize UVC '/server-admin/operations/diagnose/ping/'远程代码执行漏洞	高	暂无
CNVD-2014-02694	Acunetix Web Vulnerability Scanner 远程堆缓冲区溢出漏洞	高	暂无
CNVD-2014-02691	Festo CECX-X-C1 和 CECX-X-M1 控制器未授权访问漏洞	高	暂无
CNVD-2014-02690	Festo CECX-X-M1 控制器 FTP 后门漏洞	高	暂无
CNVD-2014-02700	Adobe Flash Player Pixel Bender 组件缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://helpx.adobe.com/security/products/flash-player/apsb14-13.html

表 3 部分高危漏洞列表

小结：本周，Microsoft 被披露存在多个安全漏洞，攻击者可利用漏洞提升本地权限或执行任意代码。此外，Apache、Cisco、Google 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，Python 被披露存在一个高危零日漏洞，攻击者可利用漏洞执行任意代码。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、Red Hat 修补 OpenShift Enterprise 产品漏洞

OpenShift 是由红帽推出的一款面向开源开发人员开放的平台即服务(PaaS)。

本周，Red Hat 修补了上述产品存在的验证绕过漏洞，避免远程攻击者向 openshift-origin-broker 发送请求，设置 X-Remote-User 头字段，然后发送请求至 passthrough 触发器，可绕过验证检查，以 OpenShift 用户账户上下文登录系统。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/45208>

本周要闻速递

1. 苹果开发者中心网站存在重大安全漏洞

据外媒报道，苹果开发者中心网站，日前被曝存在重大安全漏洞，黑客可以利用这一漏洞获取该网站所储存的大量隐私信息。也有消息称，黑客可以通过这一在上周末被发现的漏洞获取包括已注册的 iOS、Mac 和 Safari 开发者账户的开发人员、苹果零售人员、公司员工、合作伙伴甚至是少数高管的个人联系方式和信息。这一漏洞最早是苹果开发者在当地时间周六发现的，在国外科技媒体 9to5mac 获悉了这一情况后便立刻联系了苹果方面。9to5mac 表示，由于这一漏洞非常严重，因此网站无法在发现这一漏洞的第一时间公诸于众，只有在该漏洞被彻底封堵后才能够公布有关信息。

参考链接：<http://soft.zol.com.cn/451/4510211.html>

2. 微软发布紧急安全补丁修复 IE 漏洞

5 月 2 日消息，据国外媒体报道，微软周四发布了一个安全补丁来修复 IE 浏览器中的一个重要的安全漏洞。这个安全漏洞会让恶意黑客绕过 Windows 操作系统的安全保护机制。当用户访问恶意网站时，他们的计算机就会被攻破。微软表示，这次发布的安全补丁支持所有版本的 Windows 系统和 IE 浏览器，用户们只要开启自动升级功能即可。

这个升级补丁已于美东时间 5 月 1 日上午 10 点上线。此次升级还有一个值得关注的地方，那就是它将 Windows XP 系统也包括了进去。微软已于 4 月 8 日正式停止为 XP 系统提供支持服务。

参考链接：http://news.ccidnet.com/art/1032/20140502/5447405_1.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