

## 信息安全漏洞周报

2014 年 9 月 1 日-2014 年 9 月 7 日

2014 年第 36 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 133 个，其中高危漏洞 38 个、中危漏洞 82 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 122 个。本周收录的漏洞中，已有 78 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“vBulletin 'cat'参数 SQL 注入漏洞”、“WordPress 插件 Huge-IT Gallery 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 133 个漏洞。报送情况如表 1 所示。其中，奇虎 360、安天实验室、启明星辰、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、上海天泰网络技术有限公司及白帽子向 CNVD 提交了 383 个原创漏洞。

| 报送单位或个人 | 漏洞报送数量 | 原创漏洞数量 |
|---------|--------|--------|
| 奇虎 360  | 353    | 353    |
| 安天实验室   | 114    | 0      |
| 启明星辰    | 83     | 0      |
| 恒安嘉新    | 81     | 0      |
| 绿盟科技    | 64     | 0      |
| 天融信     | 60     | 0      |

|                                    |         |     |
|------------------------------------|---------|-----|
| High-Tech Bridge Security Research | 2       | 2   |
| CNCERT 福建分中心                       | 10      | 10  |
| CNCERT 山西分中心                       | 8       | 8   |
| CNCERT 湖南分中心                       | 2       | 2   |
| CNCERT 宁夏分中心                       | 1       | 1   |
| CNCERT 江西分中心                       | 1       | 1   |
| 上海天泰网络技术有限公司                       | 1       | 1   |
| 个人                                 | 5       | 5   |
| 报送总计                               | 785     | 383 |
| 录入总计                               | 133（去重） | 383 |

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 WordPress、TYPO3、IBM 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  | WordPress           | 18   | 14%  |
| 2  | TYPO3               | 11   | 8%   |
| 3  | IBM                 | 9    | 7%   |
| 4  | Mozilla             | 8    | 6%   |
| 5  | Advantech Co., Ltd. | 8    | 6%   |
| 6  | Cisco               | 7    | 5%   |
| 7  | Code Aurora Forum   | 4    | 3%   |
| 8  | Linux               | 3    | 2%   |
| 9  | SAP                 | 2    | 1%   |
| 10 | 其他                  | 63   | 48%  |

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 133 个漏洞。其中应用程序漏洞 80 个，WEB 应用漏洞 37 个，操作系统漏洞 8 个，网络设备漏洞 3 个，数据库漏洞 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   | 80   |
| WEB 应用漏洞 | 37   |

|        |   |
|--------|---|
| 操作系统漏洞 | 8 |
| 网络设备漏洞 | 3 |
| 数据库漏洞  | 3 |
| 安全产品漏洞 | 2 |

表 3 漏洞按影响类型统计表

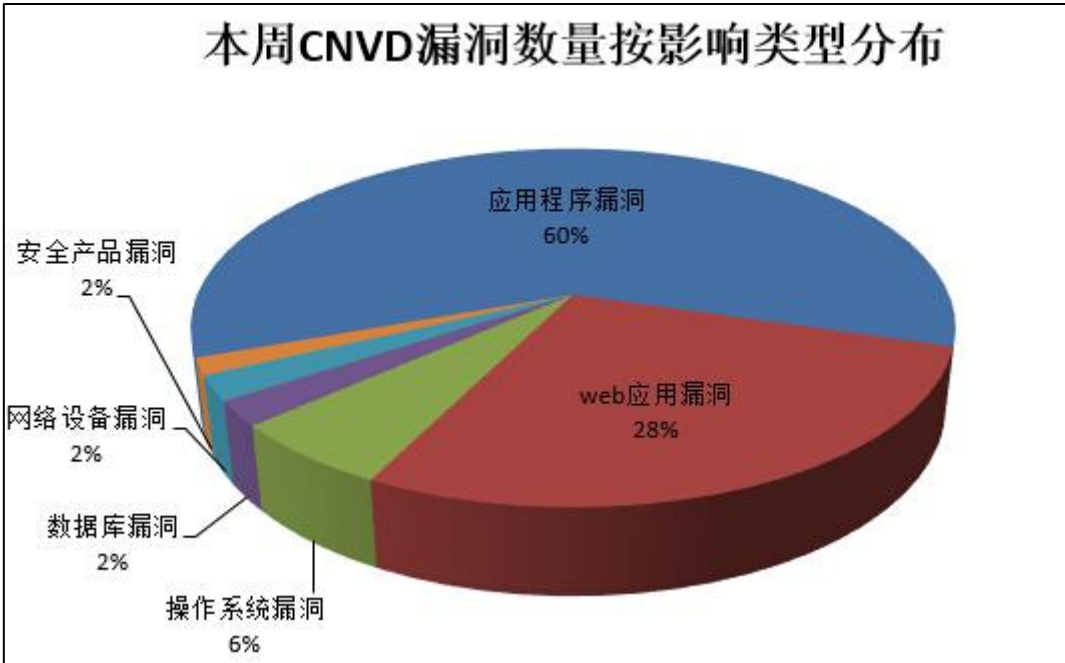


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 2 个电信行业漏洞，3 个移动互联网漏洞，8 个工控行业漏洞（如下图表所示）。

| 行业    | 漏洞编号            | 漏洞标题                                            | 危险等级 | 是否有补丁 |
|-------|-----------------|-------------------------------------------------|------|-------|
| 电信    | CNVD-2014-05344 | ARRIS Touchstone Data Gateway DG8 60P2 远程信息泄露漏洞 | 中    | 否     |
| 电信    | CNVD-2014-05401 | Cisco IOS XR Software 拒绝服务漏洞                    | 中    | 是     |
| 移动互联网 | CNVD-2014-05361 | Amazon Kindle for Android SSL 证书验证安全绕过漏洞        | 中    | 是     |
| 移动互联网 | CNVD-2014-05394 | Android Browser application 安全绕过漏洞              | 中    | 是     |
| 移动互联网 | CNVD-2014-05455 | Darinsoft Air Transfer for iOS 安全绕过漏洞           | 中    | 否     |
| 工控系统  | CNVD-2014-05416 | Advantech WebAccess 缓冲区溢出漏洞（CNVD-2014-05416）    | 高    | 否     |
| 工控系统  | CNVD-2014-05422 | Advantech WebAccess 缓冲区溢出漏洞（CNVD-2014-05422）    | 高    | 否     |
| 工控系统  | CNVD-2014-05421 | Advantech WebAccess 缓冲区溢出漏洞                     | 高    | 否     |

|      |                 |                                               |   |   |
|------|-----------------|-----------------------------------------------|---|---|
|      |                 | (CNVD-2014-05421)                             |   |   |
| 工控系统 | CNVD-2014-05423 | Advantech WebAccess 缓冲区溢出漏洞 (CNVD-2014-05423) | 高 | 否 |
| 工控系统 | CNVD-2014-05420 | Advantech WebAccess 缓冲区溢出漏洞 (CNVD-2014-05420) | 高 | 否 |
| 工控系统 | CNVD-2014-05419 | Advantech WebAccess 缓冲区溢出漏洞 (CNVD-2014-05419) | 高 | 否 |
| 工控系统 | CNVD-2014-05418 | Advantech WebAccess 缓冲区溢出漏洞 (CNVD-2014-05418) | 高 | 否 |
| 工控系统 | CNVD-2014-05417 | Advantech WebAccess 缓冲区溢出漏洞 (CNVD-2014-05417) | 高 | 否 |

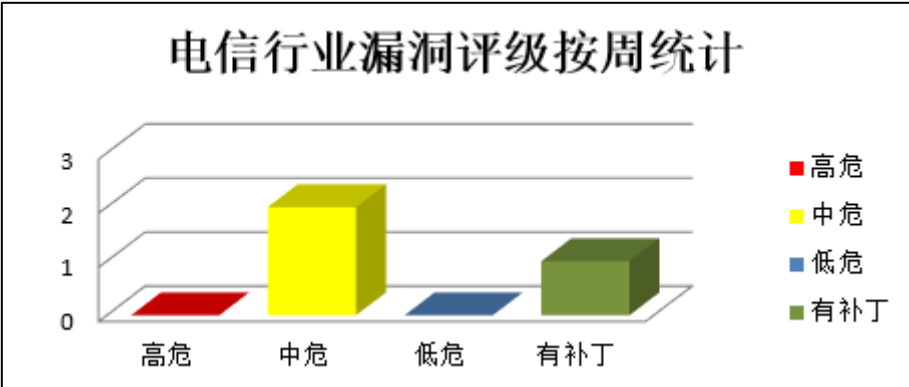


图 1 电信行业漏洞统计

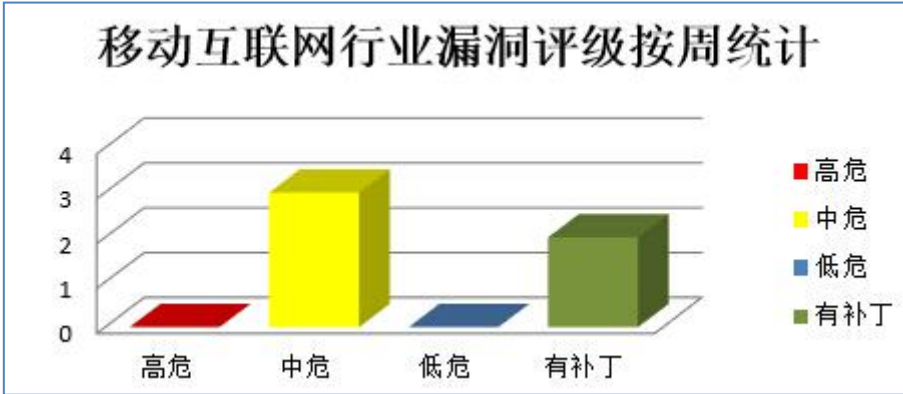


图 2 移动互联网行业漏洞统计

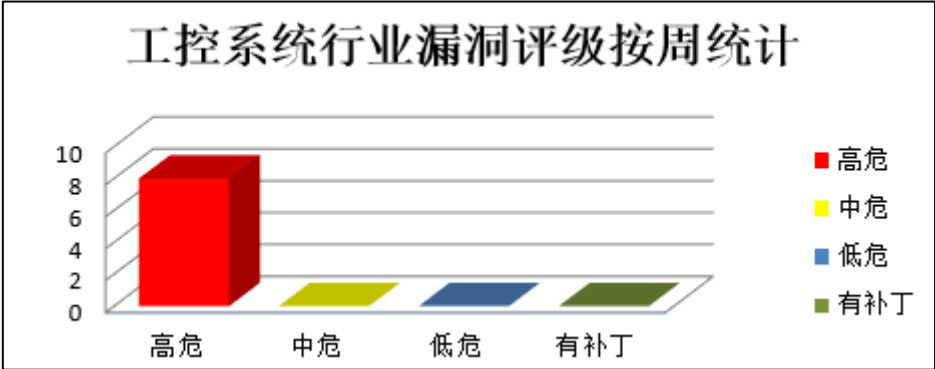


图 3 工控行业漏洞统计



## 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、Mozilla 产品安全漏洞

Mozilla Firefox/Thunderbird 是一款 Mozilla 出品的浏览器和邮件客户端。本周，上述产品被披露存在内存破坏和信息泄露漏洞，攻击者可利用漏洞在受影响的应用程序上下文执行任意代码或获取敏感信息。

CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird 内存破坏漏洞（CNVD-2014-05414、CNVD-2014-05413、CNVD-2014-05411、CNVD-2014-05410、CNVD-2014-05406、CNVD-2014-05407）、Mozilla Firefox for Android 不完整修复信息泄露漏洞、Mozilla Firefox/Thunderbird 信息泄露漏洞（CNVD-2014-05412）。除“Mozilla Firefox/Thunderbird 内存破坏漏洞（CNVD-2014-05407）、Mozilla Firefox for Android 不完整修复信息泄露漏洞、Mozilla Firefox/Thunderbird 信息泄露漏洞（CNVD-2014-05412）”外，其余漏洞的综合评级为“高危”。目前，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-2014-05414>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05413>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05411>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05410>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05406>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05407>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05415>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05412>

### 2、IBM 产品安全漏洞

IBM Business Process Manager 是一款不断积累数据的有状态产品；DB2 是 IBM 出品的一系列关系型数据库管理系统，分别在不同的操作系统平台上服务；IBM Maximo Asset Management 和 SmartCloud Control Desk (SCCD) 都是美国 IBM 公司的企业资产管理产品；IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案；SCCD 是一套统一资产和服务管理软件。IBM Worklight Foundation 是美国 IBM 公司的一套用于开发、测试、管理和保护 HTML5、混合和本机移动应用程序的解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意脚本代码、进行未经授权操作或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM Business Process Manager 和 WebSphere 任意文件上传漏洞、IBM DB2 多个产品模块 ALTER 语句处理远程栈缓冲区溢出漏洞、IBM

Business Process Manager 信息泄露漏洞（CNVD-2014-05428）、IBM Business Process Manager 和 WebSphere 安全绕过漏洞、IBM DB2/DB2 拒绝服务漏洞、IBM DB2 多个产品本地信息泄露漏洞、IBM Maximo Asset Management 和 Maximo Asset Management for SmartCloud Control Desk 跨站请求伪造漏洞、IBM Worklight and IBM Mobile Foundation 验证绕过漏洞。其中，“IBM Business Process Manager 和 WebSphere 任意文件上传漏洞、IBM DB2 多个产品模块 ALTER 语句处理远程栈缓冲区溢出漏洞”漏洞的综合评级为“高危”。目前，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-2014-05427>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05363>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05428>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05429>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05449>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05362>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05350>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05348>

### 3、Cisco 产品安全漏洞

Cisco IOS XR 是 Cisco IOS 软件家族的一员，使用基于微内核分配操作系统架构；Cisco Cloud Portal 是一款思科公司推出的相关云的解决方案；Smart Call Home 作为智能服务的关键组成部分，同时也是 SMARTnet 服务之一，已经在众多思科产品用得到应用。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、执行任意脚本代码、进行钓鱼攻击或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IOS XR Software 拒绝服务漏洞、Cisco Intelligent Automation for Cloud 远程信息泄露漏洞（CNVD-2014-05347）、Cisco Intelligent Automation for Cloud 开放重定向漏洞、Cisco Intelligent Automation for Cloud 远程信息泄露漏洞、Cisco Intelligent Automation for Cloud 任意文件上传漏洞、Cisco Transport Gateway for Smart Call Home 安全绕过漏洞、Cisco Transport Gateway for Smart Call Home 拒绝服务漏洞。其中，“Cisco IOS XR Software 拒绝服务漏洞、Cisco Intelligent Automation for Cloud 远程信息泄露漏洞（CNVD-2014-05347）”漏洞厂商已经发布了修补程序。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-2014-05401>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05347>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05339>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05338>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05337>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05332>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05331>

#### 4、TYPO3 产品安全漏洞

TYPO3 是一款开源的内容管理系统。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞进行跨站攻击、获取敏感信息或执行任意脚本代码。

CNVD 收录的相关漏洞包括：TYPO3 Flat Manager 存在未明 SQL 注入漏洞、TYPO3 CWT Frontend Edit Extension 存在未明远程代码执行漏洞、TYPO3 ke DomPDF Extension 存在未明远程代码执行漏洞、TYPO3 Address visualization with Google Maps 存在未明 SQL 注入漏洞、TYPO3 wt\_directory Extension 存在未明 SQL 注入漏洞、TYPO3 LumoNet PHP Include Extension 存在未明远程代码执行漏洞、TYPO3 LDAP Extension 信息泄露漏洞、TYPO3 Open Graph Protocol 存在未明跨站脚本漏洞。除“TYPO3 LDAP Extension 信息泄露漏洞、TYPO3 Open Graph Protocol 存在未明跨站脚本漏洞”外，其余漏洞的综合评级为“高危”。目前，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-2014-05445>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05444>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05443>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05442>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05438>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05437>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05441>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05440>

#### 5、ActualAnalyzer 'backticks'远程代码执行漏洞

ActualAnalyzer 是网站统计工具，用于监控网站流量分析。本周，ActualAnalyzer 被披露存在综合评级为“高危”的远程代码执行漏洞。攻击者可利用漏洞在受影响的应用程序上下文中执行任意命令。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-2014-05335>

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-2014-05334 | PhpWiki Ploticus 模块命令注入漏洞                        | 高    | 暂无   |
| CNVD-2014-05326 | XRMS CRM 'plugins/webform/new-form.php' SQL 注入漏洞 | 高    | 暂无   |

|                 |                                                        |   |                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CNVD-2014-05327 | XRMS CRM 'plugins/useradmin/finderuser.php'远程命令执行漏洞    | 高 | 暂无                                                                                                                                                                                                                 |
| CNVD-2014-05367 | ManageEngine DesktopCentral 不完全修复任意文件上传漏洞              | 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：<br><a href="http://www.manageengine.com">http://www.manageengine.com</a>                                                                                                         |
| CNVD-2014-05377 | Manageengine Desktop Central 任意文件上传漏洞                  | 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：<br><a href="http://www.manageengine.com/products/desktop-central/">http://www.manageengine.com/products/desktop-central/</a>                                                     |
| CNVD-2014-05376 | ManageEngine Desktop Central 任意文件上传漏洞（CNVD-2014-05376） | 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：<br><a href="http://www.manageengine.com/products/desktop-central/">http://www.manageengine.com/products/desktop-central/</a>                                                     |
| CNVD-2014-05379 | F5 Unauthenticated rsync 远程根代码执行漏洞                     | 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：<br><a href="http://support.f5.com/kb/en-us/solutions/public/15000/200/sol15236.html">http://support.f5.com/kb/en-us/solutions/public/15000/200/sol15236.html</a>                 |
| CNVD-2014-05388 | MSM camera driver 权限提升漏洞                               | 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：<br><a href="https://www.codeaurora.org/patches/quick/la/.PATCH_24430_iwoLuwW321heHwU.tar.gz">https://www.codeaurora.org/patches/quick/la/.PATCH_24430_iwoLuwW321heHwU.tar.gz</a> |
| CNVD-2014-05380 | MX-SmartTimer '/Login.aspx' SQL 注入漏洞                   | 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：<br><a href="http://www.mpexsolutions.com/solutions/workforce-on-demand/timesheets-expenses/">http://www.mpexsolutions.com/solutions/workforce-on-demand/timesheets-expenses/</a> |
| CNVD-2014-05432 | SolarWinds Log & Event Manager HyperSQL 远程代码执行漏洞       | 高 | 用户可以联系供应商获得补丁信息：<br><a href="http://www.solarwinds.com">http://www.solarwinds.com</a>                                                                                                                              |

表 3 部分高危漏洞列表

小结：本周，Mozilla 多款产品被披露存在多个漏洞，允许攻击者利用漏洞在受影响的应用程序上下文执行任意代码或获取敏感信息。此外，IBM、Cisco、TYPO3 多款产品被披露存在多个漏洞，攻击者利用漏洞可获取敏感信息、进行跨站脚本攻击、执行任意脚本代码或发起拒绝服务攻击。另外，ActualAnalyzer 被披露存在一个高危零日漏

洞。攻击者可利用漏洞在受影响的应用程序上下文中执行任意命令。建议相关用户应随时关注上述厂商主页，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 修补 Kernel 产品漏洞

Linux Kernel 是 Linux 操作系统的内核。

本周，Linux 修补了上述产品存在的拒绝服务和缓冲区溢出漏洞，避免攻击者利用漏洞发起拒绝服务攻击或执行任意代码。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/49712>  
<http://www.cnvd.org.cn/patchInfo/show/49619>

## 本周要闻速递

### 1. 微软 IE 现新安全漏洞 Windows XP 无补丁

微软发布了 2963983 安全公告，从 IE 6 到 IE 10 的浏览器都被查出一种可远程执行代码的漏洞，用户访问特别设计过的恶意网站时会遭到类似处理电子邮件链接的攻击。目前漏洞并未广泛传播。声明中微软表示：“成功利用此漏洞的攻击者可以获得当前用户的同等权限。如果当前用户登录使用了管理员权限，那么成功利用此漏洞的攻击者可以取得受影响系统的完整控制权。攻击者随后可安装程序，查看、更改或删除数据，或者创建新帐户拥有完全的用户权限。”微软表示除 XP 外的其它 Windows 用户将在一到两星期内获得 IE 补丁，不过由于 XP 已经在 4 月 8 日停止得到支持，将不会收到任何更新。

参考链接：<http://tech.hexun.com/2014-09-05/168223275.html>

### 2. 安卓浏览内核再现安全漏洞

据某报告平台报道，Android 系统浏览内核 Webkit 存在跨域漏洞，恶意网页可利用该漏洞跨站获取用户敏感信息，例如登录信息、页面内容等，基于该浏览内核的系统默认浏览器、第三方浏览器以及内置网页浏览能力的 app 都受到影响。相关报道指出，谷歌 Android 操作系统团队在漏洞公开前早已知悉，后续发行版已经修复该漏洞，但未同步修复旧版本，Android4.3 以下都在受影响范围内，覆盖了目前市面上的大部分手机，事态严重。

参考链接：<http://digi.163.com/14/0903/17/A582N18N001618JV.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](http://www.cert.org.cn)

邮箱：[vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话：010-82990999