国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 12 月 21 日-2015 年 12 月 27 日 **2015 年第 52 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**高**。

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 178 个，其中高危漏洞 53 个、中危漏洞 121 个、低危漏洞 4 个。上述漏洞中，可利用来实施远程攻击的漏洞有 160 个。本周收录的漏洞中，已有 148 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。其中互联网上出现“Wordpress Cool Video Gallery 插件命令注入漏洞”、“Cisco Prime Collaboration Assurance 默认帐户凭据漏洞”等零日漏洞，请使用相关产品的用户注意加强防范。

本周，针对 Java 反序列化远程代码执行漏洞的威胁态势仍旧不容乐观，CNVD 已经累计处置数百起境内党政机关、重要信息系统部门以及基础电信企业的漏洞案例，以 Jboss 和 Weblogic 容器服务器为主。本周，互联网上又出现了针对 Weblogic 容器的无反弹直接远程回显的攻击代码实例，对大量的 Weblogic 服务器的攻击门槛又进一步降低。

本周互联网上还披露了 Juniper Screen OS 的后门漏洞，同样会引发大规模网络攻击和远程控制的高危风险。CNVD 已经处置了数十个涉及该漏洞的党政机关、基础电信企业的漏漏洞案例，同时发布了《关于 Juniper Networks ScreenOS 后门漏洞监测和处置情况的安全公告》，详情参见 CNVD 网站公告内容：http://www.cnvd.org.cn/webinfo/show/3763

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 178 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、安天实验室、绿盟科技、天融信等单位报送数量较多。补天平台、乌云及白帽子向 CNVD 提交了 1141 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量

奇虎(补天平台)	640	640
安天实验室	109	0
绿盟科技	79	0
天融信	62	0
启明星辰	55	0
恒安嘉新	38	0
乌云	487	487
广州白狐网络科技有限公司	1	1
CNCERT 甘肃分中心	3	3
CNCERT 宁夏分中心	1	1
CNCERT 福建分中心	1	1
个人	8	8
报送总计	1484	1141
录入总计	178（去重）	1141

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、Mozilla、Xen 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	26	15%
2	Mozilla	21	12%
3	Xen	11	6%
4	IBM	9	5%
5	XMLSoft	8	4%
6	eWON	6	3%
7	HP	5	3%
8	Drupal	5	3%
9	FFmpeg	3	2%

10	其他	84	47%

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 178 个漏洞。其中应用程序漏洞 114 个，网络设备漏洞 27 个，Web 应用漏洞 24 个，安全产品漏洞 7 个，操作系统漏洞 6 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	114
网络设备漏洞	27
Web 应用漏洞	24
安全产品漏洞	7
操作系统漏洞	6

表 3 漏洞按影响类型统计表

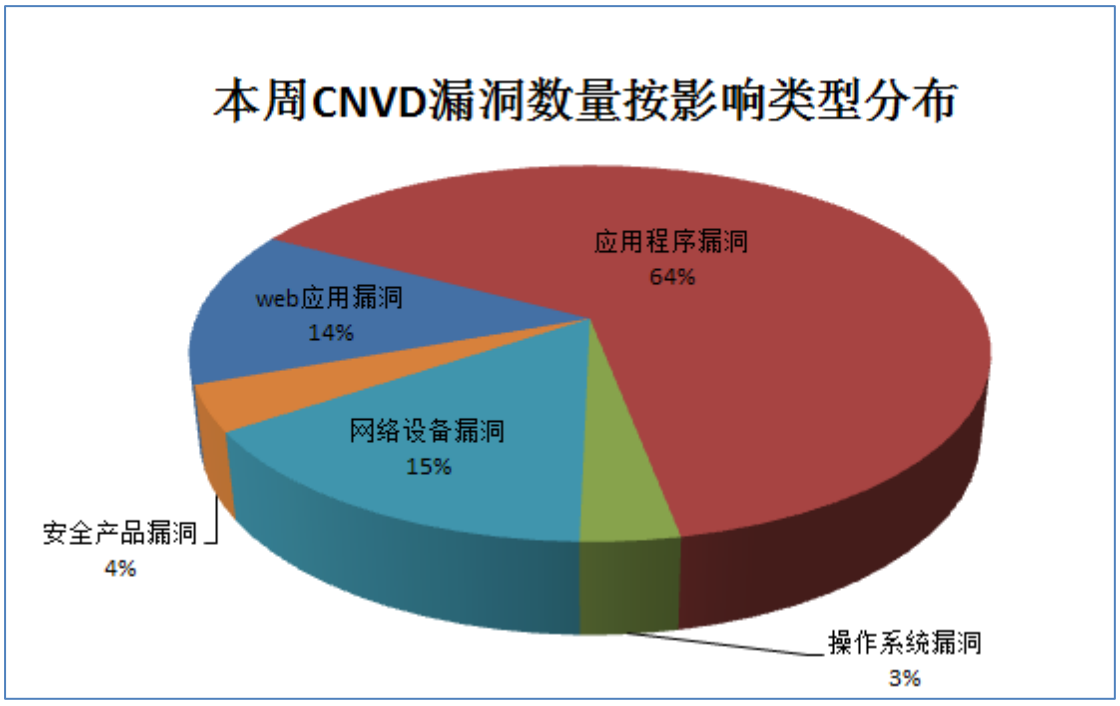

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 32 个电信行业漏洞、2 个移动互联网行业漏洞、5 个工控系统行业漏洞（如下图表所示）。其中，“IBM Tivoli Monitoring 远程代码执行漏洞、ISC BIND named 竞争条件漏洞、Wind River VxWorks 整数溢出漏洞（CNVD-2015-08443）、Schneider Electric Modicon M340 PLC BMXNOx 和 BMXPx 栈缓冲溢出漏洞”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-2015-08311	多款 Cisco IP 产品任意文件上传漏洞	中	否
电信	CNVD-2015-08335	IBM Tivoli Monitoring 远程代码执行漏洞	高	是
电信	CNVD-2015-08344	IBM WebSphere Portal 跨站脚本漏洞（CNVD-2015-08344）	中	是
电信	CNVD-2015-08365	Cisco Emergency Responder 跨站脚本漏洞（CNVD-2015-08365）	中	否
电信	CNVD-2015-08363	Cisco Unified Computing System (UCS) 拒绝服务漏洞	中	是
电信	CNVD-2015-08360	Cisco Unified Communications Manager Mobile and Remote Access 安全绕过漏洞	中	否
电信	CNVD-2015-08368	Cisco Emergency Responder Web 框架任意文件上传漏洞	中	否
电信	CNVD-2015-08367	Cisco Emergency Responder 目录遍历漏洞	中	否
电信	CNVD-2015-08366	Cisco Emergency Responder 跨站请求伪造漏洞（CNVD-2015-08366）	中	否
电信	CNVD-2015-08372	ISC BIND named 竞争条件漏洞	高	是
电信	CNVD-2015-08373	ISC BIND named 拒绝服务漏洞	中	是
电信	CNVD-2015-08374	Cisco Unified Communications Manager 拒绝服务漏洞（CNVD-2015-08374）	中	否
电信	CNVD-2015-08385	Cisco EPC3928 跨站脚本漏洞	中	否
电信	CNVD-2015-08384	Cisco EPC3928 devices with EDVA 安全机制绕过漏洞	中	否
电信	CNVD-2015-08383	Cisco DPQ3925 devices with EDVA 跨站请求伪造漏洞	中	否
电信	CNVD-2015-08393	Cisco IOS 拒绝服务漏洞（CNVD-2015-08393）	中	是
电信	CNVD-2015-08392	IBM WebSphere Application Server 信息泄露漏洞（CNVD-2015-08392）	中	是
电信	CNVD-2015-08420	Netgear G54/N150 WNR1000v3 Router 安全绕过漏洞	中	否
电信	CNVD-2015-08442	Apache Camel Java 对象反序列化漏洞	中	是
电信	CNVD-2015-08436	IBM WebSphere Portal 信息泄露漏洞（CNVD-2015-08436）	中	是
电信	CNVD-2015-08435	IBM Tivoli Storage FlashCopy Manager 和 Tivoli Storage Manager 本地提权漏洞（CNVD-2015-08435）	中	是
电信	CNVD-2015-08434	IBM Tivoli Storage FlashCopy Manager 和 Tivoli Storage Manager 本地提权漏洞	中	是
电信	CNVD-2015-08445	Cisco IOS 及 IOS XE Software IKEv1 状态机拒绝服务漏洞	中	是

电信	CNVD-2015-08450	eWON 弱会话管理漏洞	中	是
电信	CNVD-2015-08448	Motorola Solutions MOSCAD SCADA IP Gateway 跨站请求伪造漏洞	高	否
电信	CNVD-2015-08447	Motorola Solutions MOSCAD SCADA IP Gateway 任意文件下载漏洞	高	否
电信	CNVD-2015-08455	eWON 信息泄露漏洞	中	是
电信	CNVD-2015-08454	eWON 明文密码信息泄露漏洞	中	是
电信	CNVD-2015-08453	eWON 跨站脚本漏洞	中	是
电信	CNVD-2015-08452	eWON 未授权访问漏洞	中	是
电信	CNVD-2015-08451	eWON 跨站请求伪造漏洞	中	是
电信	CNVD-2015-08466	Cisco IOS XE Software 拒绝服务漏洞（CNVD-2015-08466）	中	是
移动互联网	CNVD-2015-08343	Apple iOS GANMA 应用程序安全绕过漏洞	中	是
移动互联网	CNVD-2015-08359	Apple iOS 和 Safari WebKit 信息泄露漏洞	中	是
工控系统	CNVD-2015-08443	Wind River VxWorks 整数溢出漏洞（CNVD-2015-08443）	高	是
工控系统	CNVD-2015-08448	Motorola Solutions MOSCAD SCADA IP Gateway 跨站请求伪造漏洞	高	否
工控系统	CNVD-2015-08447	Motorola Solutions MOSCAD SCADA IP Gateway 任意文件下载漏洞	高	否
工控系统	CNVD-2015-08446	Schneider Electric Modicon M340 PLC BMXNOx 和 BMXPx 栈缓冲溢出漏洞	高	是
工控系统	CNVD-2015-08469	Pacom RTU/1000 CCU/EMCS 加密弱口令漏洞	中	否

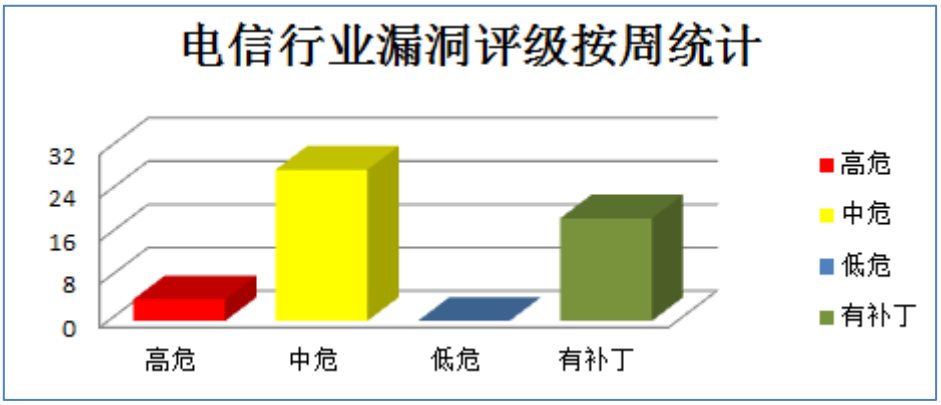

图 1 电信行业漏洞统计

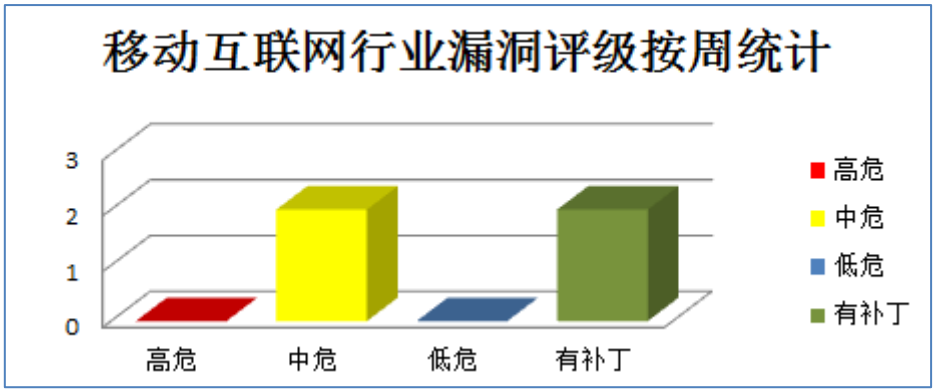

图 2 移动互联网行业漏洞统计

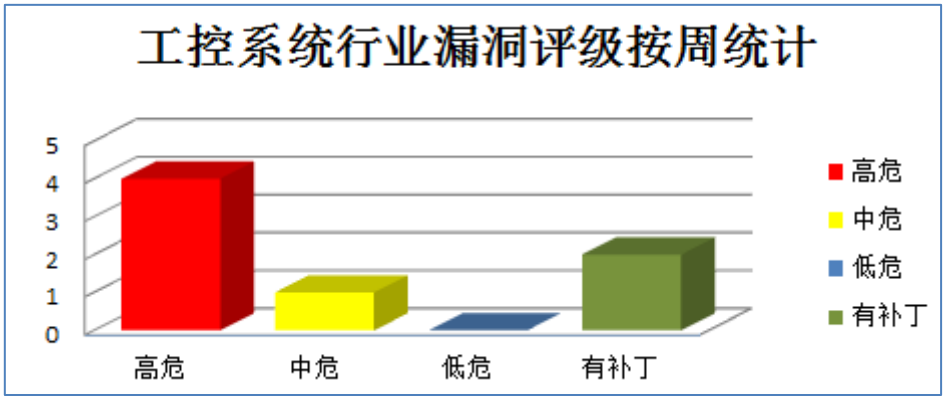

图 3 工控系统行业漏洞统计

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、 Juniper Networks 产品安全漏洞

近日，Juniper Networks 公司发布公告称其销售的部分型号防火墙产品使用的操作系统 ScreenOS 存在后门漏洞(CNVD 收录编号:CNVD-2015-08306 和 CNVD-2015-08307，对应 CVE-2015-7755 和 CVE-2015-7756)。攻击者利用上述漏洞可通过 SSH 或者 Telnet 远程管理访问设备，获取管理员权限；或可解密 NetScreen 设备的 VPN 流量，改变或删除日志条目，隐藏入侵痕迹。

CNVD 收录的相关漏洞包括：Juniper Networks ScreenOS 存在后门漏洞（CNVD-2015-08306、CNVD-2015-08307）。上述漏洞的综合评级均为“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-2015-08306

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08307

2、 Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会开发的一款开源 Web 浏览器。本周，该产品被披露存在内存错误引用、整数溢出、缓冲区溢出和拒绝服务漏洞。攻击者利用上述漏洞可执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Mozilla Firefox 缓冲区溢出漏洞（CNVD-2015-08328、CNVD-2015-08313、CNVD-2015-08322、CNVD-2015-08321）、Mozilla Firefox 整数溢出漏洞（CNVD-2015-08330）、Mozilla Firefox 内存错误引用漏洞（CNVD-2015-08331）、Mozilla Firefox 拒绝服务漏洞（CNVD-2015-08327）、Mozilla Firefox 和 Firefox ESR 缓冲区溢出漏洞。上述漏洞的综合评级均为“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-2015-08328

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08313

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08322

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08321

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08330

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08331

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08327

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08329

3、IBM 产品安全漏洞

IBM Tivoli Storage FlashCopy Manager 是一套通过集成快照功能，为关键的应用和数据库提供高级别数据保护的软件；Tivoli Storage Manager 是一套能够对电子邮件服务器自动进行数据保护的软件；IBM WebSphere Portal 是创建一个联接企业内部和外部的平台，可让员工、客户和供应商等通过该平台访问企业内部数据的解决方案；IBM WebSphere Application Server 是一款应用服务器；IBM Tivoli Monitoring（ITM）是一套系统监控软件；IBM Mashups Center 是一套用于业务人员和 IT 人员创建、发布、修改和共享 Web 应用的平台；IBM Sterling B2B Integrator 是一套集成了重要的 B2B 流程、交易和关系的软件。本周，上述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、提升权限、执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM Tivoli Storage FlashCopy Manager 和 Tivoli Storage Manager 本地提权漏洞、IBM WebSphere Portal 信息泄露漏洞（CNVD-2015-08436）、IBM WebSphere Portal 跨站脚本漏洞（CNVD-2015-08344）、IBM Tivoli Storage FlashCopy Manager 和 Tivoli Storage Manager 本地提权漏洞（CNVD-2015-08435）、IBM WebSphere Application Server 信息泄露漏洞（CNVD-2015-08392）、IBM Tivoli Monitoring 远程代码执行漏洞、IBM Mashups Center 拒绝服务漏洞、IBM Sterling B2B Integrator 本地信息泄露漏洞（CNVD-2015-08354）。其中，“IBM Tivoli Monitoring 远程代码执行漏洞”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。C

NVD 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-2015-08434

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08436

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08344

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08435

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08392

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08335

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08355

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08354

4、HP 产品安全漏洞

HP HPE Helion Eucalyptus 是美国惠普（HP）公司的一套开源的私有云解决方案；HP StoreOnce Backup System 是一套基于磁盘的备份系统；HP Insight Control Server Provisioning 是一套服务器管理工具，该工具支持管理服务器的健康状况、部署和快速迁移服务器等。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞可执行未授权访问、进行跨站脚本和跨站请求伪造攻击和执行任意代码。

CNVD 收录的相关漏洞包括：HP HPE Helion Eucalyptus 未授权访问漏洞、HP StoreOnce Backup System 跨站请求伪造漏洞、HP Insight Control Server Provisioning 信息泄露漏洞、HP StoreOnce Backup System 跨站脚本漏洞、HP StoreOnce Backup System 任意代码执行漏洞。其中，“HP StoreOnce Backup System 任意代码执行漏洞”的综合评级为“高”危。目前，厂商已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-2015-08465

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08423

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08421

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08425

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08424

5、Apache TomEE 'EjbObjectInputStream'任意命令执行漏洞

Apache TomEE 是美国阿帕奇软件基金会所研发的一款 Java EE 服务器。本周，Apache TomEE 被披露存在任意命令执行漏洞。攻击者可利用该漏洞执行任意命令。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-2015-08409

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-2015-08340	libpng 堆缓冲区溢出漏洞	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://www.libpng.org/pub/png/libpng.html
CNVD-2015-08377	Joomla!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：https://developer.joomla.org/security-centre/635-20151214-core-directory-traversal-2.html
CNVD-2015-08378	Joomla!目录遍历漏洞（CNVD-2015-08378）	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://developer.joomla.org/security-centre/634-20151214-core-directory-traversal.html
CNVD-2015-08380	Joomla!任意代码执行漏洞	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://developer.joomla.org/security-centre/630-20151214-core-remote-code-execution-vulnerability.html
CNVD-2015-08381	Joomla! Framework Session package 任意代码执行漏洞	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://developer.joomla.org/security-centre/637-20151205-session-remote-code-execution-vulnerability.html
CNVD-2015-08390	Google Chrome 存在多个未明漏洞（CNVD-2015-08390）	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://code.google.com/p/chromium/issues/detail?id=534994
CNVD-2015-08388	Blink 拒绝服务漏洞（CNVD-2015-08388）	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://codereview.chromium.org/1463433002/
CNVD-2015-08387	Google Chrome 拒绝服务漏洞（CNVD-2015-08387）	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://code.google.com/p/chromium/issues/detail?id=548273
CNVD-2015-08404	Xen PV Backend Driver 远程代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://xen.xensource.com/
CNVD-2015-08405	Zen Cart 任意文件包含漏洞	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://www.zen-cart.com/showthread.php?218914-Security-Patches-for-v

			1-5-4-November-2015

表 3 部分高危漏洞列表

小结：本周，Juniper Networks 公司发布公告称其销售的部分型号防火墙产品使用的操作系统 ScreenOS 存在后门漏洞，攻击者利用上述漏洞可通过 SSH 或者 Telnet 远程管理访问设备，获取管理员权限；或可解密 NetScreen 设备的 VPN 流量。此外，Mozilla、IBM、HP 多款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、执行未授权访问、提升权限、执行任意代码、发起跨站攻击和拒绝服务攻击等。另外，Apache TomEE 被披露存在一个高危漏洞，攻击者可利用该漏洞执行任意命令。建议相关用户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、Schneider Electric 修补 Modicon M340 和 ProClima 产品漏洞

Schneider Electric Modicon M340 PLC BMXNOx 和 BMXPx 都是法国施耐德电气（Schneider Electric）公司的可编程控制器产品。GoAhead Web Server 是一款嵌入式 Web 服务器；Schneider Electric ProClima 是一款热力计算软件。

本周，Schneider Electric 修补了上述产品存在的栈缓冲溢出和拒绝服务漏洞，避免攻击者利用漏洞执行任意代码和发起拒绝服务攻击。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/68892

http://www.cnvd.org.cn/patchInfo/show/68764

本周要闻速递

1. 4000 个微笑表情能导致 WhatsApp 崩溃

一位独立研究员，Indrajeet Bhuyan 报告了存在于 WhatsApp 中的一个新漏洞，通过利用该漏洞，任何人都可以远程使 WhatsApp 崩溃，而他们需要做的仅仅是向目标用户发送将近 4000 个表情符号。该漏洞影响全球约 10 亿 WhatsApp 用户。

参考链接：http://www.freebuf.com/news/90730.html

2. iOS 越狱设备木马 TinyV 出现

近日网络安全公司 Palo Alto Networks 公司的安全研究人员 Claud Xiao 发布了一篇内容为分析新木马“TinyV”的文章。Palo Alto Networks 公司的安全研究人员在今年 10 月份发现了该木马文件，当时其实发现了一个恶意的负载文件瞄准了 iOS 的越狱设备，并发现该文件属于一个名为“TinyV”的新型 iOS 木马家族。最近，有中国用户

指出他们的设备受到了这个恶意软件的影响。目前该公司发现这个木马只是针对越狱的 iOS 设备，该恶意木马文件已经被重新打包并植入到一些 iOS 应用中，而这些 iOS 应用往往可以通过多个第三方渠道进行下载。

参考链接：http://www.freebuf.com/news/90281.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