

信息安全漏洞周报

2016 年 06 月 20 日-2016 年 06 月 26 日

2016 年第 26 期

本周漏洞态势研判情况

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 178 个，其中高危漏洞 57 个、中危漏洞 113 个、低危漏洞 8 个。漏洞平均分为 6.34 分。本周收录的漏洞中，涉及 0day 漏洞 16 个（占 9%）。其中互联网上出现“FineCMS 后台模板管理存在设计逻辑漏洞”等零日漏洞，请使用相关产品的用户注意加强防范。此外，本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1091 个，与上周（1380 个）环比下降 21%。

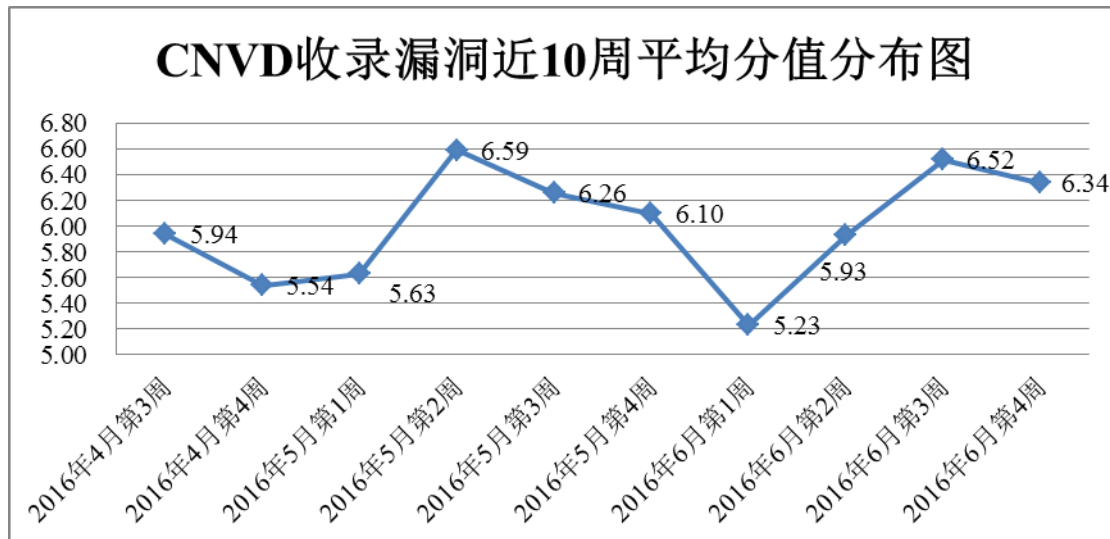


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 8 家成员单位、合作伙伴及企业用户、个人用户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，安天实验室、天融信、恒安嘉新、启明星辰等单位报送数量较多。补天平台、乌云、漏洞盒子、西安四叶草信息技术有限公司、深圳市

深信服电子科技有限公司、广州圣辉信息技术有限公司及其他个人白帽子向 CNVD 提交了 1091 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)	420	420
安天实验室	164	0
天融信	127	0
恒安嘉新	123	29
启明星辰	101	0
绿盟科技	98	0
中国电信集团系统集成有限责任公司	77	0
H3C	8	0
乌云	470	470
漏洞盒子	24	24
西安四叶草信息技术有限公司	111	111
深圳市深信服电子科技有限公司	14	14
广州圣辉信息技术有限公司	3	3
CNCERT 上海分中心	1	1
CNCERT 宁夏分中心	1	1
CNCERT 江西分中心	1	1
个人	17	17
报送总计	1760	1091
录入总计	178（去重）	1091

表 1 成员单位上报漏洞统计表



本周漏洞按类型和厂商统计

本周，CNVD 收录了 178 个漏洞。其中应用程序漏洞 134 个，网络设备漏洞 19 个，操作系统漏洞 15 个， Web 应用漏洞 9 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	134
网络设备漏洞	19
操作系统漏洞	15
web 应用漏洞	9
安全产品漏洞	1

表 2 漏洞按影响类型统计表

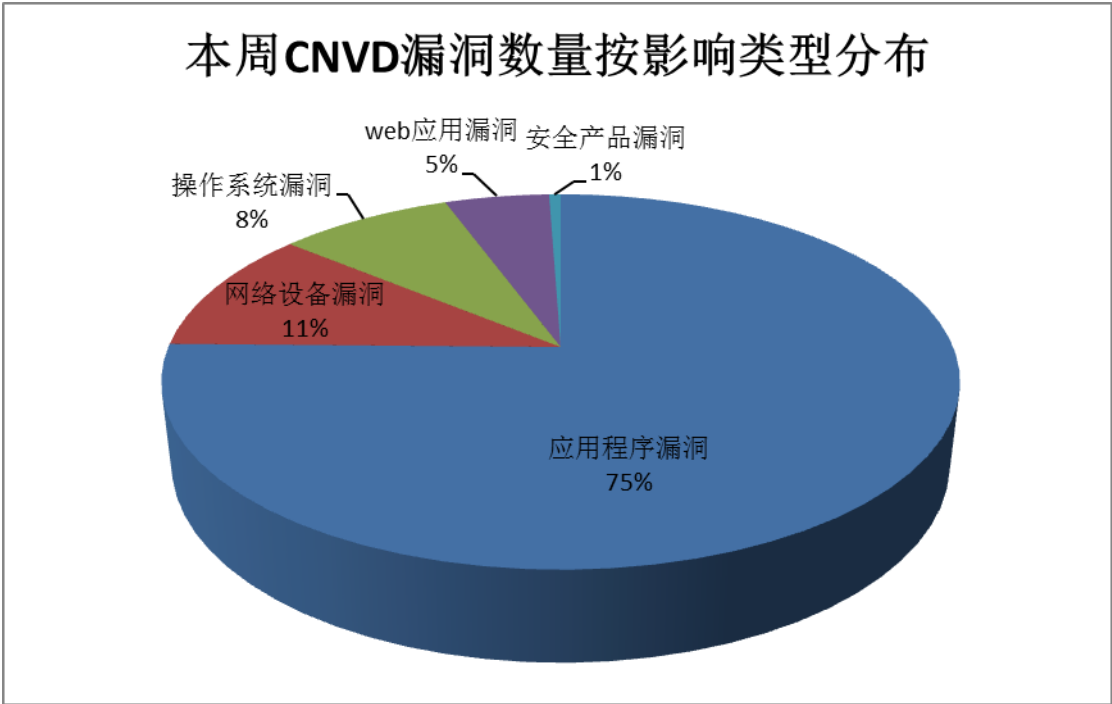


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、libarchive、Cisco 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Adobe	43	24%
2	libarchive	23	13%
3	Cisco	13	7%
4	IBM	11	6%
5	Microsoft	5	3%
6	Red Hat	5	3%
7	ImageMagick	5	3%

8	Apple	4	2%
9	CloudBees	3	2%
10	其他	66	37%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，5 个移动互联网行业漏洞，2 个工控系统行业漏洞（如下图所示）。其中，“Android 权限提升漏洞（CNVD-2016-04110）、Android NVIDIA 摄像头驱动权限提升漏洞、Android NVIDIA 摄像头驱动权限提升漏洞（CNVD-2016-04112）、Weiphp 系统存在 SQL 注入漏洞”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，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：<http://telecom.cnvd.org.cn/>

移动互联网行业漏洞链接：<http://mi.cnvd.org.cn/>

工控系统行业漏洞链接：<http://ics.cnvd.org.cn/>

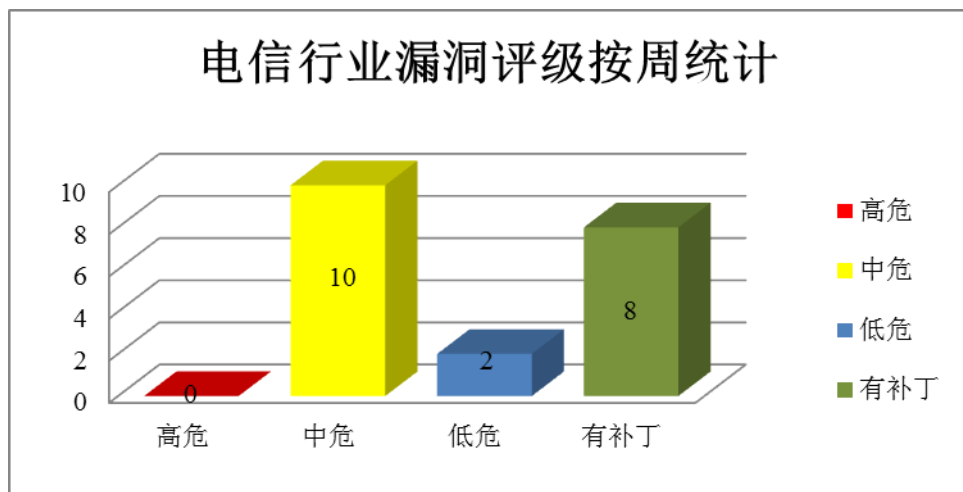


图 3 电信行业漏洞统计

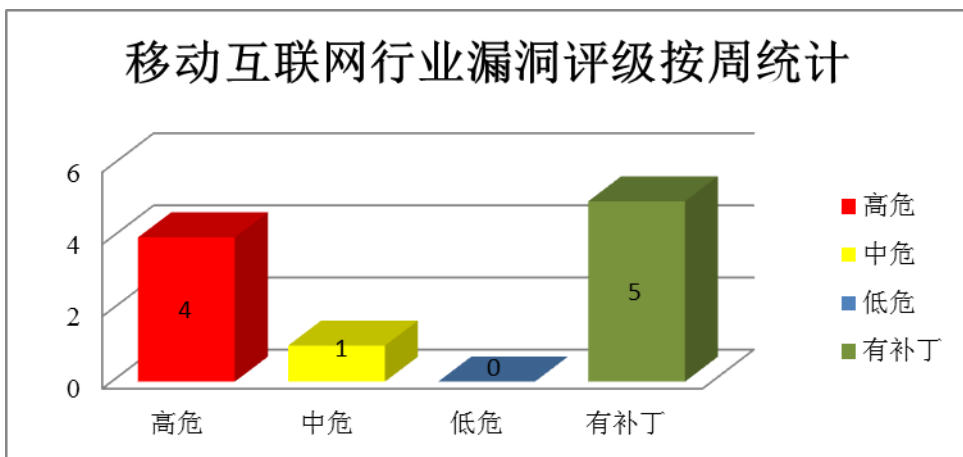


图 4 移动互联网行业漏洞统计

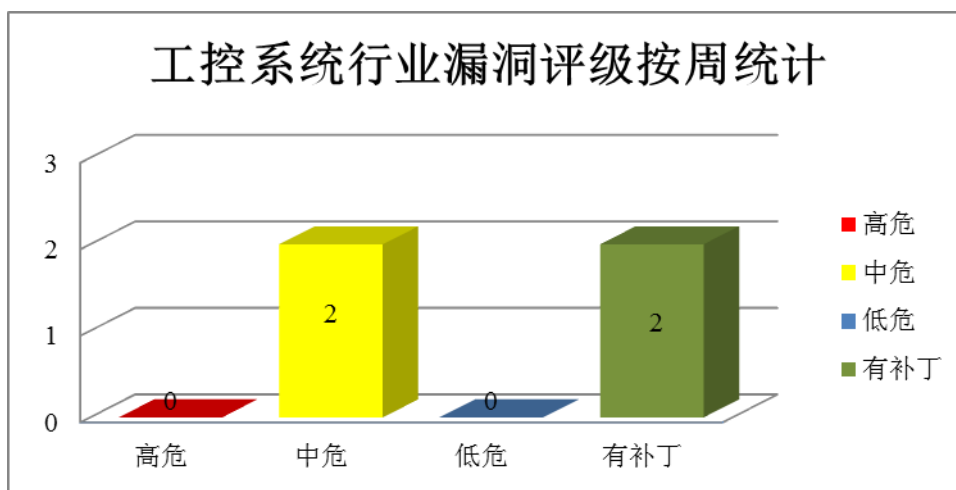


图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Adobe 产品安全漏洞

Adobe Flash Player 是一款多媒体播放器产品；Adobe ColdFusion 是一款动态 Web 服务器产品，其运行的 CFML 是针对 Web 应用的一种程序设计语言。本周，上述产品被披露存在内存破坏、内存错误引用和跨站脚本漏洞，攻击者可利用漏洞进行跨站脚本攻击和执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 存在未明内存破坏漏洞（CNVD-2016-04201）、Adobe Flash Player 存在未明内存错误引用漏洞（CNVD-2016-04200）、Adobe Flash Player 内存破坏漏洞（CNVD-2016-04103、CNVD-2016-04102、CNVD-2016-04101、CNVD-2016-04100）、Adobe Flash Player 存在未明漏洞（CNVD-2016-04099）、Adobe ColdFusion 跨站脚本漏洞（CNVD-2016-04109）。其中，除“Adobe ColdFusion 跨站脚本漏洞（CNVD-2016-04109）”外，其余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-2016-04201>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04200>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04103>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04102>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04101>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04100>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04099>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04109>

2、libarchive 产品安全漏洞

libarchive 是一个多格式存档和压缩库。本周，上述产品被披露存在越边界读取和内存读取漏洞，攻击者可利用漏洞造成越边界读取和无效的内存读取。

CNVD 收录的相关漏洞包括：libarchive TAR 解析器堆越边界读取漏洞、libarchive mtree 解析器越边界读取漏洞、libarchive ar 解析器栈越边界读取漏洞、libarchive LHA/LZH 解析器堆越边界读取漏洞、libarchive mtree 解析器堆越边界读取漏洞、libarchive 堆越边界读取漏洞、libarchive RAR 解析器堆越边界读取漏洞、libarchive CPIO 解析器内存读取漏洞等。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-2016-04249>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04252>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04253>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04254>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04257>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04258>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04178>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04219>

3、Cisco 产品安全漏洞

Cisco IOS、IOS XE 是美国思科（Cisco）公司为其网络设备开发的操作系统。Cisco IP Phone 8800 Series 是美国思科（Cisco）公司的 8000 系列 IP 电话产品。该产品提供了语音、视频功能。Cisco Unified Contact Center Enterprise 是美国思科（Cisco）公司的一套基于 IP 的联系中心组件。该组件在 IP 基础设施上提供了智能联系路由、呼叫处理、网络到桌面计算机电话集成（CTI）和多通道联系管理功能。Cisco AsyncOS on Email Security Appliance（ESA）是美国思科（Cisco）公司的一套运行在电子邮件安全设备（ESA）中的操作系统。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、进行未授权操作、执行跨站脚本攻击和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IOS XE SNMP 子系统拒绝服务漏洞、Cisco IOS XE on cBR-8 Converged Broadband Router IOS XE 拒绝服务漏洞、Cisco IOS 拒绝服务漏洞（CNVD-2016-04224、CNVD-2016-04228）、Cisco IP Phone 8800 Series 未授权访问漏洞、Cisco IP Phone 8800 Series 目录遍历漏洞、Cisco Email Security Appliance AsyncOS 安全绕过漏洞、Cisco ASR 5000 Series Packet Data Network Gateway 拒绝服务漏洞等。其中，除“Cisco Email Security Appliance AsyncOS 安全绕过漏洞”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-2016-04183>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04215>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04224>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04228>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04236>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04235>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04304>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04269>

4、IBM 产品安全漏洞

IBM QRadar SIEM 是美国 IBM 公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。IBM Security QRadar Incident Forensics 是美国 IBM 公司的一套安全取证调查软件。IBM Maximo Asset Management 是美国 IBM 公司的一套综合性资产生命周期和维护管理解决方案。IBM MessageSight 是美国 IBM 公司的一款专为机器对机器（m2m）和移动环境而设计的消息传递设备。IBM Personal Communications 是美国 IBM 公司的一套专用于 Microsoft Windows 的主机通信和终端仿真软件包。IBM Rational Collaborative Lifecycle Management（CLM）等都是美国 IBM 公司的产品。IBM WebSphere Portal 是美国 IBM 公司的产品。IBM WebSphere Portal 是一套企业门户软件。IBM TRIRIGA Application Platform 是美国 IBM 公司的一套用于部署 TRIRIGA 应用的技术平台。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、发起拒绝服务攻击、实施跨站脚本攻击等。

CNVD 收录的相关漏洞包括：IBM QRadar SIEM 敏感信息获取漏洞、IBM Security QRadar Incident Forensics 未授权访问漏洞、IBM Maximo Asset Management 跨站脚本漏洞、IBM MessageSight 任意命令执行漏洞、IBM Personal Communications 未授权访问漏洞、IBM Jazz Foundation 信息泄露漏洞、IBM WebSphere Portal 跨站请求伪造漏洞（CNVD-2016-04105）、IBM TRIRIGA Application Platform 跨站脚本漏洞（CNVD-2016-04104）等。其中，“IBM MessageSight 任意命令执行漏洞”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。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-2016-04293>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04292>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04237>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04222>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04113>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04108>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04105>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04104>

5、Wolf CMS Metasploit 模块任意文件上传漏洞

Wolf CMS 是一套内容管理系统 (CMS)。Metasploit 是其中的一个安全漏洞检测工具组件。本周, Wolf CMS 被披露存在任意文件上传漏洞。允许攻击者利用漏洞上传任意文件。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-2016-04297>

更多高危漏洞如表 4 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-2016-04098	Red Hat OpenStack Platform 设计漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题, 补丁获取链接: https://access.redhat.com/errata/RHSA-2016:1222
CNVD-2016-04110	Android 权限提升漏洞 (CNVD-2016-04110)	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://source.android.com/security/bulletin/2016-06-01.html
CNVD-2016-04111	Android NVIDIA 摄像头驱动权限提升漏洞	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://source.android.com/security/bulletin/2016-06-01.html
CNVD-2016-04112	Android NVIDIA 摄像头驱动权限提升漏洞 (CNVD-2016-04112)	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://source.android.com/security/bulletin/2016-06-01.html
CNVD-2016-04188	Expat XML 解析器拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: https://sourceforge.net/p/expat/code_git/ci/07cc2fcacf81b32b2e06aa918df51756525240c0/
CNVD-2016-04204	Linux kernel 'key_reject_and_link()'拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: http://www.kernel.org/
CNVD-2016-04203	Python 注入任意 HTTP 头漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: https://bugs.python.org/issue22928
CNVD-2016-04202	Python zipimport 模块堆溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: https://bugs.python.org/issue26171
CNVD-2016-04230	SolarWinds Virtualization Manager 权限获取漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题, 详情请关注厂商主

			页： http://www.solarwinds.com/
CNVD-2016-04261	Google Chrome 存在未明漏洞 (CNVD-2016-04261)	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://googlechromereleases.blogspot.com/2016/06/stable-channel-update_16.html

表 4 部分重要高危漏洞列表

小结：本周，Adobe 产品被披露存在内存破坏、内存错误引用和跨站脚本漏洞，攻击者可利用漏洞进行跨站脚本攻击和执行任意代码。此外，libarchive、Cisco、IBM 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞获得敏感信息、越边界读取、执行任意代码或发起拒绝服务攻击等。另外，Wolf CMS 被披露存在任意文件上传漏洞。允许攻击者利用漏洞上传任意文件。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。

本周漏洞要闻速递

1. 开源压缩库 Libarchive 曝高危漏洞

最近 Libarchive 又被曝出存在安全漏洞——Libarchive 是个开源压缩库，为各种不同文件档案格式准备的。Libarchive 的应用范围非常广，因此，所以大量项目自然也就受到了影响，如 Debian Linux、FreeBSD，还有诸多文件压缩工具。这次发现的漏洞包括：Libarchive 处理 7-Zip 文件时可能发生整数溢出的问题（CVE-2016-4300），还有处理 Mtree 文件时缓冲区溢出（CVE-2016-4301）、处理 RAR 文件时堆溢出（CVE-2016-4302）。很显然，这些都是相当危险的安全漏洞，攻击者可利用这些漏洞在感染的设备上远程执行代码。

参考链接：<http://www.freebuf.com/news/107566.html>

2. Android 安全开发之 ZIP 文件目录遍历

因为 ZIP 压缩包文件中允许存在“../”的字符串，攻击者可以利用多个“../”在解压时改变 ZIP 包中某个文件的存放位置，覆盖掉应用原有的文件。如果被覆盖掉的文件是动态链接 so、dex 或者 odex 文件，轻则产生本地拒绝服务漏洞，影响应用的可用性，重则可能造成任意代码执行漏洞，危害用户的设备安全和信息安全。比如近段时间发现的“寄生兽”漏洞、海豚浏览器远程命令执行漏洞、三星默认输入法远程代码执行漏洞等都与 ZIP 文件目录遍历有关。

参考链接：<http://www.freebuf.com/articles/terminal/107585.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