

信息安全漏洞周报

2017 年 09 月 18 日-2017 年 09 月 24 日

2017 年第 39 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**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 325 个，其中高危漏洞 129 个、中危漏洞 182 个、低危漏洞 14 个。漏洞平均分为 6.27。本周收录的漏洞中，涉及 0day 漏洞 90 个（占 28%），其中互联网上出现“Cisco DPC3939 固件任意命令执行漏洞”、“NexusPHP SQL 注入漏洞（CNVD-2017-27285）”等零日代码攻击漏洞。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 1162 个，与上周（1029 个）环比增长 13%。

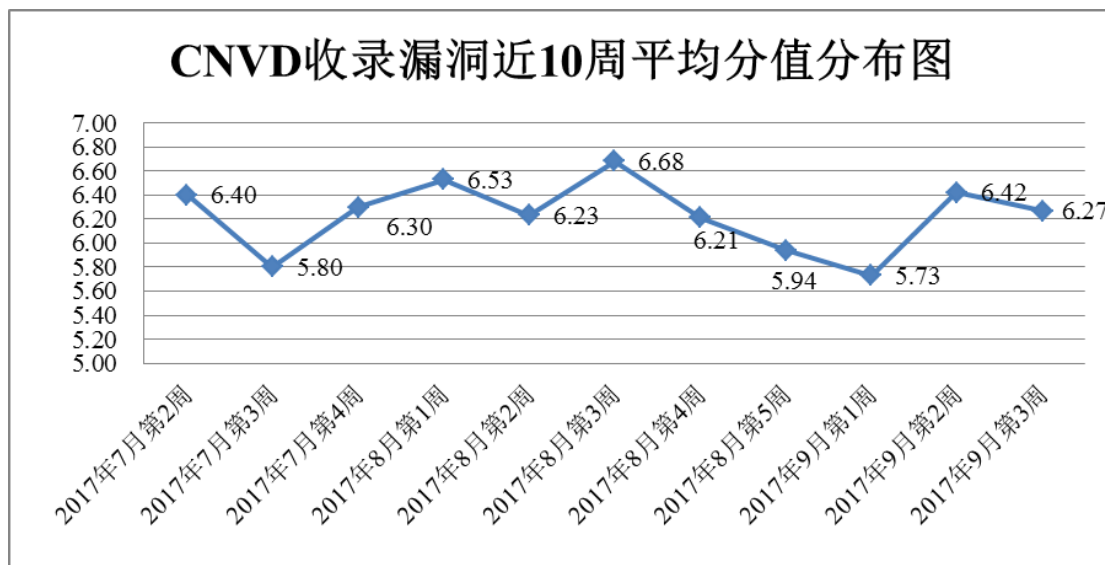


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 16 家成员单位、企业用户及个人用户报送了本周收录的全部 325 个漏洞。报送情况如表 1 所示。其中，恒安嘉新、H3C、安天实验室、华为技术有限公司、天融信等单位报送数量较多。四川虹微技术有限公司（子午攻防实验室）、深圳市鼎安天下

信息科技有限公司、中新网络信息安全股份有限公司、邹平九零冰讯网络科技有限公司、上海彝众信息技术有限公司、广州软云计算机科技有限公司及其他个人白帽子向 CNVD 提交了 1162 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
天融信	395	1
360 网神	307	307
H3C	288	0
安天实验室	214	0
恒安嘉新	197	2
华为技术有限公司	196	6
漏洞盒子	170	170
东软	120	0
启明星辰	101	4
中国电信集团系统集成有 限责任公司	90	12
北京数字观星科技有限公 司	88	0
绿盟科技	74	0
杭州安恒信息技术有限公 司	50	0
厦门服云信息科技有限公 司	22	0
南京铱迅信息技术股份有 限公司	1	1
北京无声信息技术有限公 司	1	0
四川虹微技术有限公司 (子午攻防实验室)	96	96
中新网络信息安全股份有 限公司	15	15
江苏同袍信息科技有限公 司	7	7
深圳市鼎安天下信息科技 有限公司	4	4

上海观安信息技术股份有限公司	3	3
成都思维世纪科技有限公司	2	2
广州软云计算科技有限公司	2	2
北京智游网安科技有限公司	1	1
CNCERT 广东分中心	1	1
CNCERT 浙江分中心	1	1
个人	527	527
报送总计	2973	1162
录入总计	325（去重）	1162

表 1 漏洞报送情况统计表



本周漏洞按类型和厂商统计

本周，CNVD 收录了 325 个漏洞。其中应用程序漏洞 229 个，web 应用漏洞 41 个，网络设备漏洞 29 个，操作系统漏洞 26 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	229
web 应用漏洞	41
网络设备漏洞	29
操作系统漏洞	26

表 2 漏洞按影响类型统计表

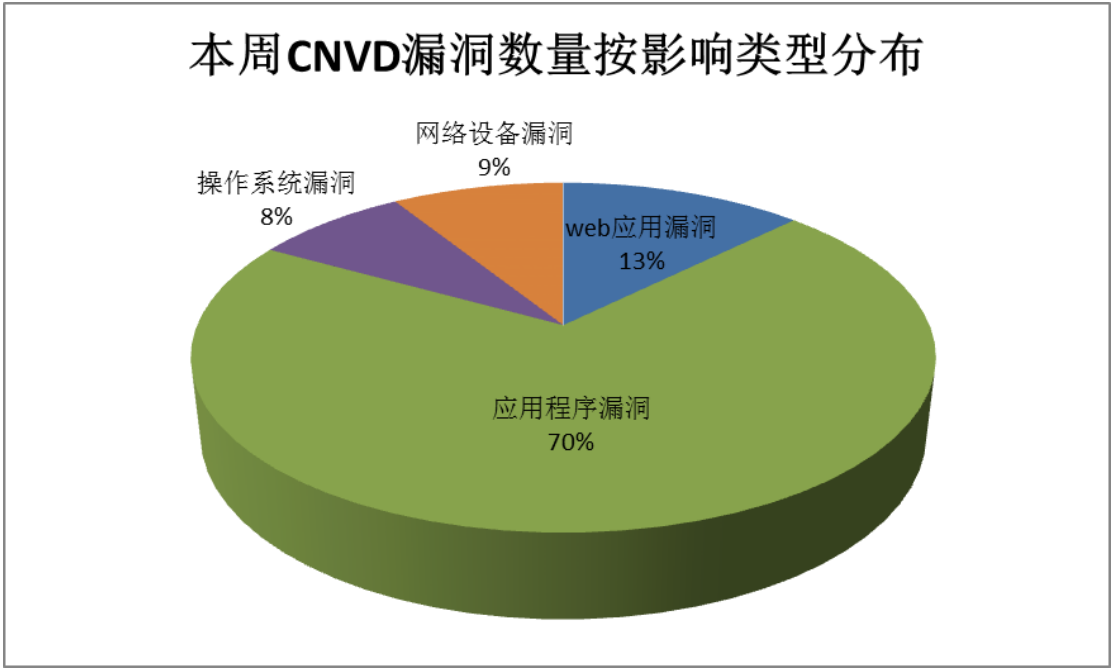


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Tcpdump、Google 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	Oracle	42	13%
2	Tcpdump	41	13%
3	Google	18	6%
4	Cisco	14	4%
5	Microsoft	10	3%
6	SMA	10	3%
7	IBM	9	3%
8	Apache	8	2%
9	Synology	8	2%
10	其他	165	51%

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 6 个电信行业漏洞，33 个移动互联网行业漏洞，5 个工控系统行业漏洞（如下图所示）。其中，“Ctek SkyRouter 身份验证绕过漏洞、Digium Asterisk GUI OS 命令注入漏洞、iniNet Solutions GmbH SCADA Webserver 未授权访问漏洞、

Apache Tomcat 信息泄露漏洞（CNVD-2017-27471）、Google Android Qualcomm 组件拒绝服务漏洞”等漏洞的综合评级为“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/>

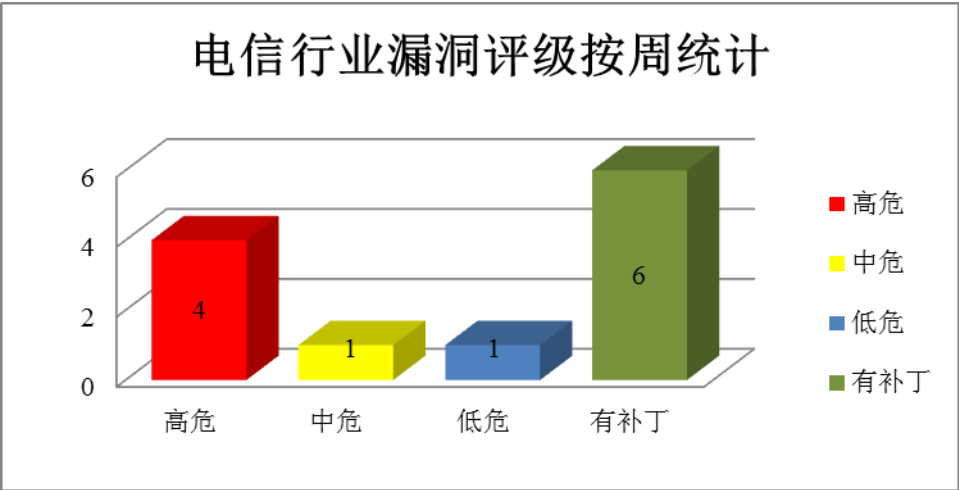


图 3 电信行业漏洞统计

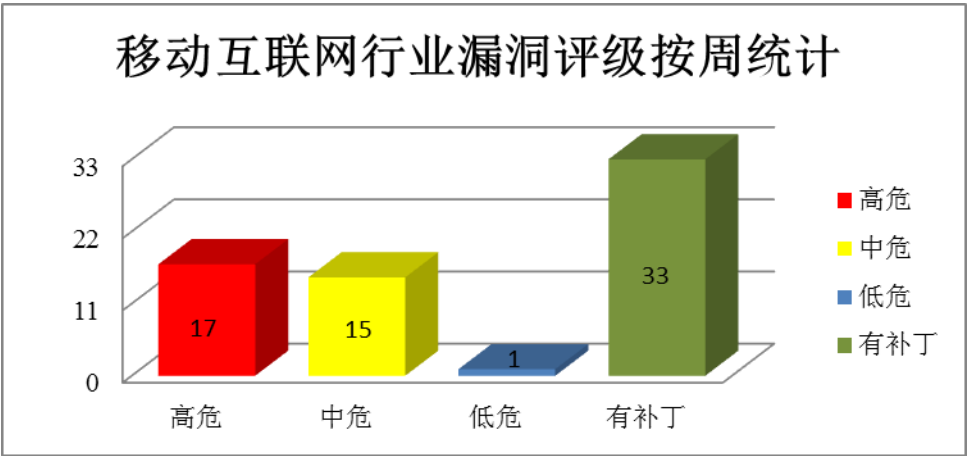


图 4 移动互联网行业漏洞统计

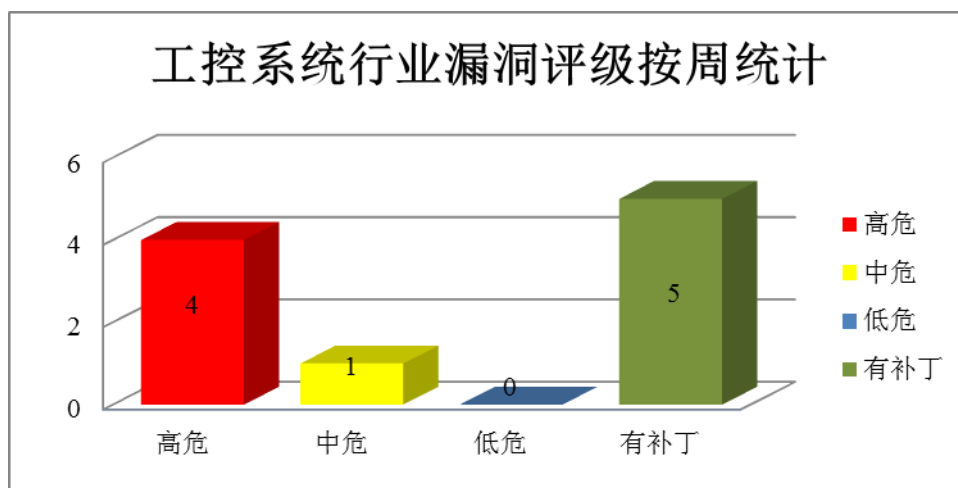


图 5 工控系统行业漏洞统计

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、Apache Tomcat 存在多个漏洞

Tomcat 是 Apache 软件基金会开发一个免费的开放源代码的 Web 应用服务器。本周，该产品被披露存在信息泄露与远程代码执行漏洞，攻击者可利用漏洞获取敏感信息或执行任意代码。

CNVD 收录的相关漏洞包括：Apache Tomcat 远程代码执行漏洞（CNVD-2017-27472）、Apache Tomcat 信息泄露漏洞（CNVD-2017-27471）。上述漏洞的综合评级为“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-2017-27472>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27471>

2、Spring AMQP 与 Spring Data REST 存在远程代码执行漏洞

Spring AMQP 是基于 Spring 框架的 AMQP 消息解决方案，Spring Data REST 可以在 Spring Data 存储库之上构建超媒体驱动的 REST Web 服务。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Pivotal Spring AMQP 远程代码执行漏洞、Pivotal Spring Data REST 远程代码执行漏洞。上述漏洞的综合评级为“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-2017-27969>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27968>

3、Tcpdump 产品安全漏洞

Tcpdump 是 Tcpdump 团队开发的一套运行在命令行下的嗅探工具。NFS parser 是其中的一个网络文件系统解析器。AODV parser 是其中的一个按需路由协议解析器。本周，该产品被披露存在堆缓冲区溢出和远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Tcpdump 缓冲区溢出漏洞（CNVD-2017-27596、CNVD-2017-27741）、Tcpdump NFS 解析器缓冲区溢出漏洞（CNVD-2017-27750、CNVD-2017-27746）、Tcpdump NFS 解析器缓冲区溢出漏洞、Tcpdump AODV 解析器缓冲区溢出漏洞、Tcpdump ARP 解析器缓冲区溢出漏洞、Tcpdump BEEP 解析器缓冲区溢出漏洞。上述漏洞的综合评级为“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-2017-27596>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27741>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27750>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27746>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27594>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27749>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27739>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27742>

4、Google 产品安全漏洞

Android 是美国谷歌公司和开放手持设备联盟共同开发的一套以 Linux 为基础的开源操作系统。Qualcomm 是使用在其中的一个美国高通公司的设备专用的高通组件。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞发起拒绝服务攻击或执行任意代码等。

CNVD 收录的相关漏洞包括：Google Android Qualcomm 组件存在未明漏洞（CNVD-2017-27865、CNVD-2017-27866、CNVD-2017-27867、CNVD-2017-27868、CNVD-2017-27869）、Google Android Qualcomm 组件缓冲区溢出漏洞（CNVD-2017-27564）、Google Android Qualcomm 组件拒绝服务漏洞、Google Android Qualcomm 组件远程代码执行漏洞。上述漏洞的综合评级为“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-2017-27865>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27866>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27867>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27868>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27869>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27564>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27563>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-27566>

5、Brother DCP-J132W 拒绝服务漏洞

Brother DCP-J132W 是 Brother 推出的打印机。本周，Brother 被披露存在远程控制漏洞，远程攻击者可通过发送大量 HTTP 数据包而导致打印机挂起（破坏其网络连接）。目前，厂商尚未发布漏洞修补程序。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-2017-27958>

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-2017-27276	LOYTEC LVIS-3ME 相对路径遍历漏洞	高	用户可联系供应商获得补丁信息： https://www.loytec.com/support/download/
CNVD-2017-27275	LOYTEC LVIS-3ME 远程代码执行漏洞	高	用户可联系供应商获得补丁信息： https://www.loytec.com/support/download/
CNVD-2017-27274	LOYTEC LVIS-3ME 跨站脚本漏洞	高	用户可联系供应商获得补丁信息： https://www.loytec.com/support/download/
CNVD-2017-27273	LOYTEC LVIS-3ME 未授权访问漏洞	高	用户可联系供应商获得补丁信息： https://www.loytec.com/support/download/
CNVD-2017-27463	Linux Kernel 'btrfs/ctree.c' 本地权限提升漏洞	高	用户可联系供应商获得补丁信息： https://www.kernel.org/
CNVD-2017-27466	Linux kernel 内存破坏漏洞（CNVD-2017-27466）	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.kernel.org/
CNVD-2017-27850	Dahua IP camera 堆栈缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息： http://www.dahuasecurity.com/firmware_161.html
CNVD-2017-27944	IP Messenger for Win 不可信搜索路径漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://jvn.jp/en/jp/JVN86724730/index.html
CNVD-2017-27945	Baidu IME 不可信搜索路径漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://jvn.jp/en/jp/JVN17788774/index.html
CNVD-2017-27946	libsndfile psf_binheader_writelf 本地权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://jvn.jp/en/jp/JVN17788774/index.html

7-27943	函数堆缓冲区溢出漏洞		注更新： https://github.com/erikd/libsndfile/issues/292
---------	------------	--	---

表 4 部分重要高危漏洞列表

小结：本周，Apache Tomcat 被披露存在信息泄露与远程代码执行漏洞，攻击者可利用漏洞获取敏感信息或执行任意代码。此外，Pivotal Software、Tcpdump、Google 多款产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息、执行任意代码或发起拒绝服务攻击等。另外，Brother 被披露存在远程控制漏洞，远程攻击者可通过发送大量 HTTP 数据包而导致打印机挂起（破坏其网络连接）。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. Optionsbleed 漏洞泄露 Apache Server 的内存信息

安全研究员 Hanno Böck 发现，部分 Apache 服务器可能因 Optionsbleed 漏洞（CVE-2017-9798）泄漏服务器内存信息。实际上这个漏洞和 OpenSSL 的心脏滴血问题有相似的地方，攻击者都可以查询服务器并向 Apache 服务器骗取数据。目前该漏洞原因已经探明，评级为中危，影响的范围有限，运行 Apache Web 服务器的用户请升级至最新版本并安装补丁。。

参考链接：<http://www.freebuf.com/vuls/148525.html>

2. WordPress 的 Display Widgets 插件存在恶意代码

Display Widgets 是 WordPress 一款显示插件。该插件的 2.6.1 到 2.6.3 版本存在恶意代码，可导致用户的 IP 地址、UA 标识等数据上传到第三方特定服务器。目前，WordPress 官方已停用 Display Widgets 2.6.1 到 2.6.3 版本。已安装 Display Widgets 插件的用户可通过查看插件主文件中的版本号确定是否受此影响，如受到此安全问题影响，请尽快卸载此插件。

参考链接：<http://www.freebuf.com/news/147887.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