

信息安全漏洞周报

2017 年 12 月 04 日-2017 年 12 月 10 日

2017 年第 50 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 480 个，其中高危漏洞 158 个、中危漏洞 278 个、低危漏洞 44 个。漏洞平均分为 5.88。本周收录的漏洞中，涉及 0day 漏洞 84 个（占 18%），其中互联网上出现“Samsung SRN-1670D Web Viewer 任意文件上传漏洞、WatchGuard Hexis HawkEye G 跨站请求伪造漏洞”零日代码攻击漏洞。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 648 个，与上周（698 个）环比减少 7%。

CNVD收录漏洞近10周平均分分布图

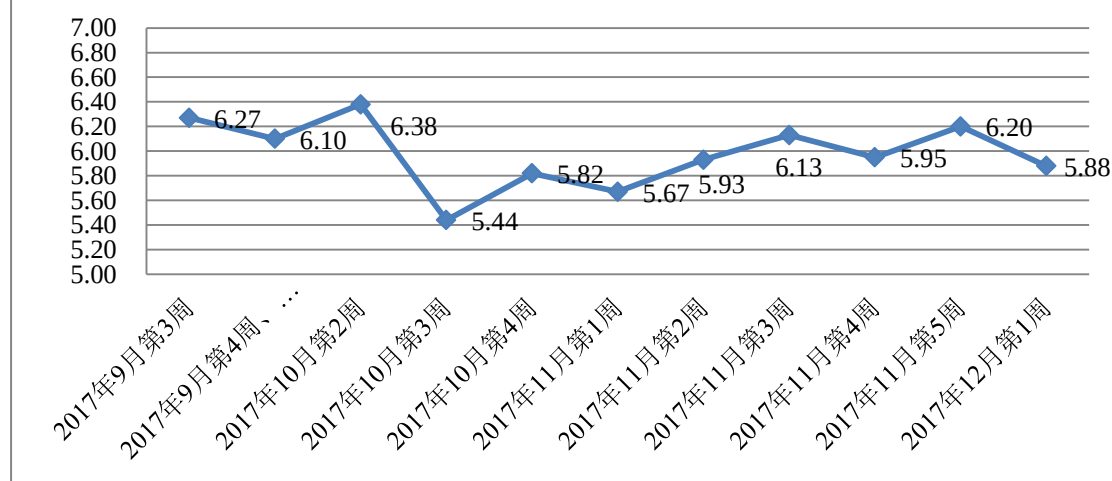


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，天融信、华为技术有限公司、安天实验室、H3C、恒安嘉新等单位报送数量较多。中新网络信息安全股份有限公司、四川虹微技术有限公司（子午攻防实验室）、南京联成科技发展股份有限公司、江苏君立华域信息安全技术

有限公司、杭州默安科技有限公司、福建榕基软件股份有限公司、邹平九零冰讯网络科技有限公司及其他个人白帽子向 CNVD 提交了 648 个以事件型漏洞为主的原创漏洞。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
天融信	209	11
360 网神	199	199
华为技术有限公司	196	0
安天实验室	180	0
H3C	176	0
恒安嘉新	133	0
绿盟科技	108	0
启明星辰	77	4
中国电信集团系统集成有 限责任公司	68	0
漏洞盒子	51	51
杭州安恒信息技术有限公 司	39	0
知道创宇	4	0
中新网络信息安全股份有 限公司	13	13
四川虹微技术有限公司 (子午攻防实验室)	8	8
南京联成科技发展股份有 限公司	4	4
江苏君立华域信息安全技 术有限公司	3	3
杭州默安科技有限公司	1	1
福建榕基软件股份有限公 司	1	1
邹平九零冰讯网络科技有 限公司	1	1
CNCERT 广东分中心	6	6

CNCERT 新疆分中心	4	4
CNCERT 海南分中心	2	2
CNCERT 吉林分中心	2	2
CNCERT 浙江分中心	2	2
个人	336	336
报送总计	1823	648

本周漏洞按类型和厂商统计

本周，CNVD 收录了 480 个漏洞。其中应用程序漏洞 283 个，web 应用漏洞 96 个，操作系统漏洞 51 个，网络设备漏洞 41 个，安全产品漏洞 5 个，数据库漏洞 4 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序漏洞	283
web 应用漏洞	96
操作系统漏洞	51
网络设备漏洞	41
安全产品漏洞	5
数据库漏洞	4

本周CNVD漏洞数量按影响类型分布

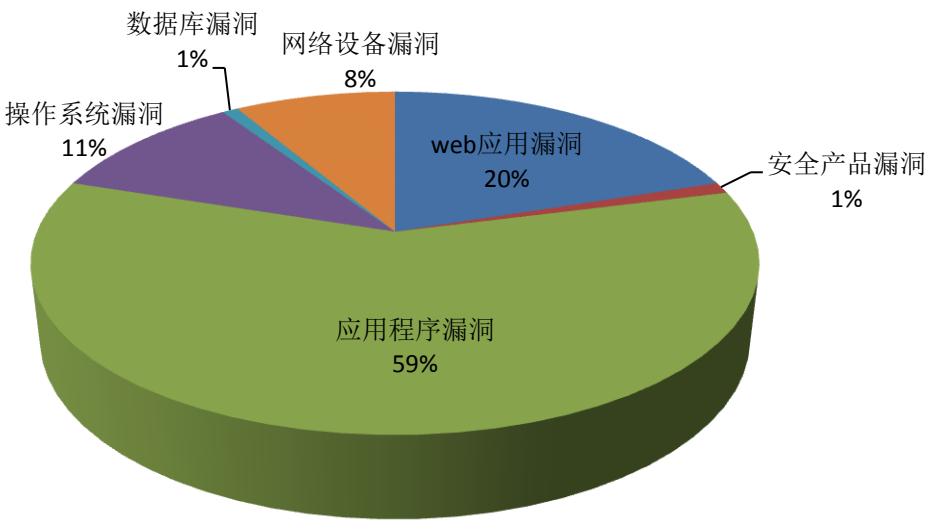


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Cisco、Catalyst IT 等多家厂商的产品，部

分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Google	63	13%
2	Cisco	37	8%
3	Catalyst IT	26	5%
4	Adobe	22	5%
5	Schneider Electric	16	4%
6	GNU	7	1%
7	上海软众网络科技有限公司	7	1%
8	EximiousSoft	6	1%
9	CloudBees	5	1%
10	其他	291	61%

本周行业漏洞收录情况

本周,CNVD 收录了 36 个电信行业漏洞,90 个移动互联网行业漏洞(如下图所示)。其中,“PostgreSQL 内存破坏漏洞、PostgreSQL 远程权限提升漏洞、Google Android Kernel Qualcomm 组件权限提升漏洞、Google Android System 权限提升漏洞、Google Android NVIDIA 组件权限提升漏洞”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/>

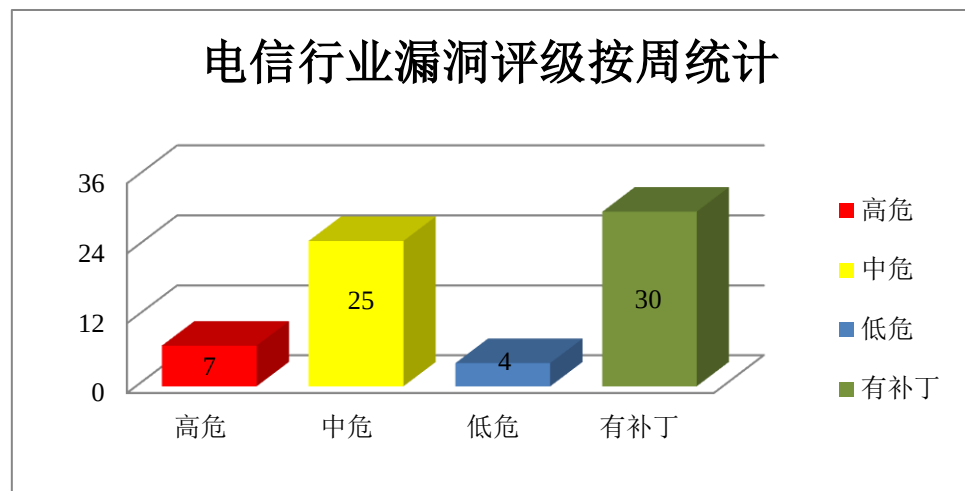


图 3 电信行业漏洞统计

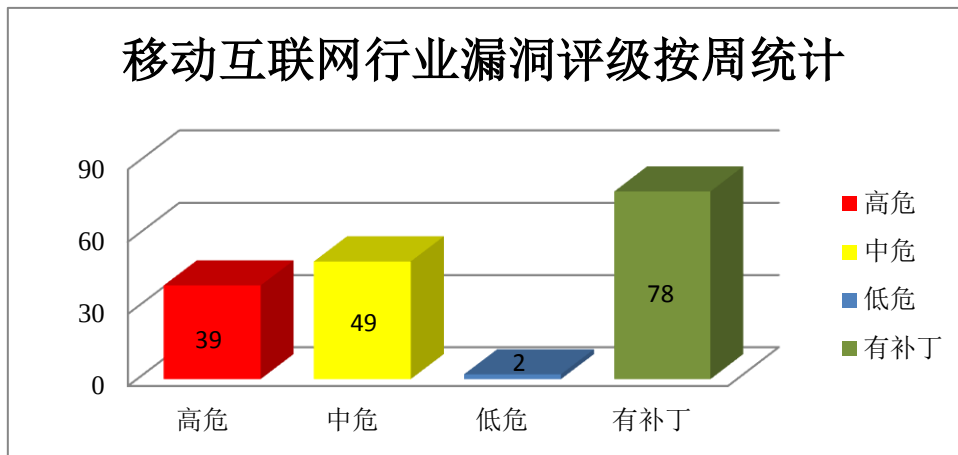


图 4 移动互联网行业漏洞统计

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、Google 产品安全漏洞

安卓（Android）是一种基于 Linux 的自由及开放源代码的操作系统。本周，该产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android Qualcomm 组件权限提升漏洞（CNVD-2017-36521、CNVD-2017-36522、CNVD-2017-36523、CNVD-2017-36524、CNVD-2017-36525、CNVD-2017-36526、CNVD-2017-36527、CNVD-2017-36528）。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-2017-36521>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36522>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36523>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36524>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36525>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36526>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36527>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36528>

2、Adobe 产品安全漏洞

Adobe Acrobat 和 Reader 是美国奥多比公开发的 PDF 文件处理程序。本周，上述产品被披露存在越界读漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 越界读漏洞（CNVD-2017-36595、CNVD-2017-36596、CNVD-2017-36597、CNVD-2017-36598、CNVD-2017-36599、

CNVD-2017-36600、CNVD-2017-36601、CNVD-2017-36602)。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-2017-35860>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35861>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35862>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35863>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35864>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35865>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35866>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35867>

3、Cisco 产品安全漏洞

Cisco Multilayer Director Switches 是美国思科（Cisco）公司的一款交换机产品。Nexus 2000 Series Fabric Extenders 是一款 Nexus 2000 系列阵列扩展器。本周，上述产品被披露存在命令注入、安全绕过和未授权访问漏洞，攻击者可利用漏洞注入任意命令、绕过安全限制或未授权读取数据等。

CNVD 收录的相关漏洞包括：多款 Cisco 产品 Cisco NX-OS System Software 命令注入漏洞、多款 Cisco 产品 Cisco NX-OS System Software 命令注入漏洞（CNVD-2017-36139、CNVD-2017-36153、CNVD-2017-36141、CNVD-2017-36152）、多款 Cisco 产品 Cisco NX-OS System Software 安全绕过漏洞、多款 Cisco 产品 Cisco NX-OS System Software 签名绕过漏洞、多款 Cisco 产品 Cisco NX-OS System Software 未授权访问漏洞。其中“多款 Cisco 产品 Cisco NX-OS System Software 命令注入漏洞、多款 Cisco 产品 Cisco NX-OS System Software 命令注入漏洞（CNVD-2017-36139、CNVD-2017-36153）、多款 Cisco 产品 Cisco NX-OS System Software 未授权访问漏洞”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-2017-36155>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36139>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36153>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36141>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36152>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36156>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36151>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36140>

4、GNU 产品安全漏洞

GNU Binutils 是一组用于创建和管理二进制程序、对象文件、库、配置文件数据及程序集源代码的编程工具。本周，该产品被披露存在缓冲区溢出和拒绝服务漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：GNU Binutils Binary File Descriptor 库缓冲区溢出漏洞、GNU Binutils 拒绝服务漏洞（CNVD-2017-36671、CNVD-2017-36672、CNVD-2017-36673、CNVD-2017-36674、CNVD-2017-36675、CNVD-2017-36676）。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-2017-36470>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36671>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36672>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36673>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36674>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36675>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-36676>

5、Philips Hue Bridge BSB002 public API 安全绕过漏洞

Philips Hue Bridge BSB002 是荷兰飞利浦(Philips)公司的一套智能家庭照明系统。本周，Philips 被披露存在安全绕过漏洞，攻击者可利用该漏洞读取 API 密钥，绕过 pushlink 保护机制并完全控制连接的配件。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-2017-36358>

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-2017-36160	Apache Traffic Server 访问绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://issues.apache.org/jira/browse/TS-2677
CNVD-2017-36207	Catalyst Mahara 认证绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://bugs.launchpad.net/mahara/+bug/1580399
CNVD-2017-36208	Catalyst Mahara 访问控制漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://bugs.launchpad.net/mahara/+bug/1577251
CNVD-2017-36209	Catalyst Mahara 重复会话头漏	高	厂商已发布漏洞修复程序，请及时关

7-36209	洞		注更新： https://bugs.launchpad.net/mahara/+bug/1570744
CNVD-2017-36279	chromium-browser WebGL 堆溢出漏洞	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://seclists.org/bugtraq/2017/Nov/21
CNVD-2017-36282	chromium-browser Skia 组件堆溢出漏洞	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://seclists.org/bugtraq/2017/Nov/21
CNVD-2017-36380	MultiTech FaxFinder 信任管理漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： http://www.multitech.com/
CNVD-2017-36407	PostgreSQL 远程权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://www.postgresql.org/about/news/1801/
CNVD-2017-36408	PostgreSQL 内存破坏漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://www.postgresql.org/about/news/1801/
CNVD-2017-36505	CMS Made Simple 服务端模板注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： http://www.cmsmadesimple.org/

表 4 部分重要高危漏洞列表

小结：本周，Google 被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。此外，Adobe、Cisco、GNU 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意代码或发起拒绝服务攻击等。另外，Philips 被披露存在安全绕过漏洞，攻击者可利用该漏洞读取 API 密钥，绕过 pushlink 保护机制并完全控制连接的配件。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. RSA 认证 SDK 中被曝两个严重漏洞

根据安全研究人员透露的信息，输入验证漏洞（CVE-2017-14377）存在于 RSA 的软件之中，而这个软件专用于为 Apache 提供基于 Web 的身份认证功能。由于 RSA 的 ApacheWeb 服务器认证代理中存在一个“输入验证问题”，因此才导致了这个认证绕过漏洞存在。另一个严重的安全漏洞存在于 RSA 的身份认证代理 SDK（C 语言版）中，这也就意味着任何部署了这个 SDK 的系统都将会受到这个漏洞的影响。研究人员表示，8.5 版本和 8.7 版本的 SDK（RSA）中存在一个错误处理漏洞（CVE-2017-14378）。这个漏洞将影响 TCP 异步模式实现，如果攻击者能够触发这个错误处理漏洞，他们将能够

绕过目标系统中的身份认证限制。

参考链接: <http://www.freebuf.com/news/156369.html>

2. PayPal 子公司 TIO Networks 被曝数据泄露

经证实, PayPal 的一家加拿大子公司 TIO Networks 曝出严重安全漏洞, 攻击者入侵了存储重要用户信息的服务器, 受影响人数约 160 万人。受数据泄露事故影响, TIO Networks 已于 11 月 10 日暂停运营, 着手调查泄露事件。该公司尚未透露哪些数据遭到泄露, 但根据其支付系统的特性推断, 攻击者获取用户个人信息以及财务信息并非难事。据悉, TIO Networks 公司已公开表达了歉意, 并表示会加强 TIO 系统安全性、保护用户信息安全。在事故调查的同时, PayPal 已经与消费者信用报告机构展开合作, 为客户免费提供信用监测成员资格。

参考链接: <http://www.freebuf.com/news/156122.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: 010-82991537